Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.3, August : 2024

CANVAST : CAN BUS SECURITY ANALYSIS AND ATTACK TYPE CLASSIFICATION WITH MINIMAL OVERHEAD

M. Kumar, Assistant Professor, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India
C.R. Balamurugan, Professor, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India
R.Elavarasi, Associate Professor, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India
M.Gokulraj, G. Ajith Kumar, K. Guruprasath UG SCHOLAR, Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India

Abstract— In spite of the fact that investigate has appeared vulnerabilities and inadequacies of the controller region arrange transport (CAN transport) and proposed options, the CAN transport convention is still the industry standard and display in most vehicles. Due to its helplessness to potential interlopers that can ruin execution or indeed take control of the vehicles, much work has center on identifying interruptions on the CAN transport. In any case, most writing does not give components to reason around, or react to the assaults so that the frame work can proceed to execute securely in spite of the gate crasher. This letter proposes a low-overhead strategy to consequently classify interruptions into predefined sorts once recognized. Our system:1) bunches messages of the same assaults into squares; 2) extricates important highlights from each square; and 3) predicts the sort of assault employing a lightweight classifier show. The introductory models portrayed in this letter appear an precision of up to 99.16% inside the primary 50ms of the assault, permitting the framework to rapidly respond to the interruption some time recently the noxious on-screen character can conclude their assault. We accept this letter lays the foundation for vehicles to have specialized runtime responses based on the assault sort.

Keywords: ***Attack sort classification, controller range organize, implanted frameworks.***

I. INTRODUCTION

"CANVAST: CAN Bus Security Analysis and Attack Type Classification with Minimal Overhead" is a research project or paper focused on the security of Controller Area Network (CAN) bus systems, commonly used in vehicles and industrial control systems. The paper likely introduces CANVAST as a methodology or tool designed to analyze the security of CAN bus networks. It emphasizes minimal overhead, meaning that the security analysis doesn't significantly impact the performance or normal operation of the CAN bus. Key components of the paper include a section which provides an overview of the importance of securing CAN bus systems due to their widespread use in vehicles and industrial settings. It may discuss potential vulnerabilities and the need for effective security measures. The paper introduces CANVAST as a specific approach or tool for analysing CAN bus security. It may explain the methodology used, including any algorithms, techniques, or technologies involved. This part details how CANVAST achieves minimal overhead, meaning that the security analysis doesn't significantly impact the performance or normal operation of the CAN bus. This is crucial in real-world applications where system performance is critical. The paper likely discusses different types of attacks that CAN bus systems may be vulnerable to, such as spoofing, replay attacks, or denial of service (DoS) attacks. It may also describe how CANVAST classifies and identifies these attack types. This section presents the results of experiments conducted using CANVAST. It may include metrics such as detection accuracy, false positives, and false negatives, demonstrating the effectiveness of the approach. Finally, the paper concludes with a summary of findings, implications for CAN bus security, and potential areas for future research or improvements to CANVAST. Overall, "CANVAST: CAN Bus Security Analysis and Attack Type Classification with Minimal Overhead" addresses the critical need for securing CAN bus systems and introduces a methodology or tool to achieve this goal

efficiently and effectively.

LOCoCAT (Low-Overhead Classification of CAN Bus Attack Types) is a research project that focuses on classifying intrusions in the Controller Area Network (CAN) bus, which is commonly used in vehicles for communication between different electrical component units (ECUs). The CAN bus protocol, despite being an industry standard, is still vulnerable to attacks from malicious actors. Since messages on the CAN bus are neither encrypted nor signed, an intruder with access to the bus can read all shared messages and even send their own messages. Most existing Intrusion Detection Systems (IDSs) stop at the detection stage, without analysing how to respond to ongoing attacks. LOCoCAT aims to address this limitation by classifying intrusions into predefined types once detected. Key features of LOCoCAT includes grouping messages where LOCoCAT groups the messages related to the same attack into blocks. Feature extraction is done by extracting relevant features from each block. Lightweight classifier model is done to predict the type of attack using a lightweight classifier model. Initial models in LOCoCAT achieved an accuracy of up to 99.16% within the first 50 milliseconds of an attack.

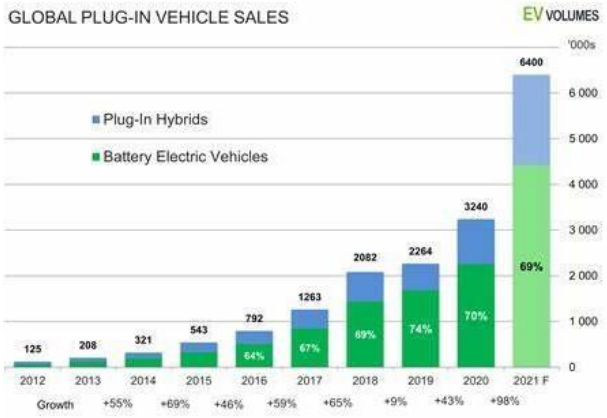

Fig. 1 Investments on EV

Figure 1 depicts about the high investment of Electric Vehicle with respect to the sales of other vehicles. It also shows a peak in hybrid vehicles due to the rise in security ailments done in the electric vehicles and about the adaptability for the current scenario in the world.

II. EXISTING METHOD

The Controller Area Network (CAN) bus protocol is a robust and widely used communication standard primarily employed in automotive and industrial applications. Its key advantage lies in its ability to facilitate communication between multiple electronic control units (ECUs) within a system, enabling real- time data exchange even in demanding environments. CAN bus offers advantages such as high reliability, low cost, and deterministic performance, making it ideal for safety-critical systems like those found in automobiles. Additionally, its multi-master architecture allows for easy integration of new devices into existing networks without causing significant disruptions. However, CAN bus also has its limitations. One notable disadvantage is its lack of built-in security features, which leaves it vulnerable to various cyber threats such as spoofing, replay attacks, and unauthorized access.

Additionally, its maximum data rate of 1 Mbps may be insufficient for certain high-bandwidth applications, necessitating the use of supplementary protocols or higher- speed alternatives. Despite these drawbacks, the widespread adoption and proven track record of CAN bus make it a cornerstone technology in modern automotive and industrial systems, albeit one that requires careful consideration of security measures and potential performance limitations.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.3, August : 2024

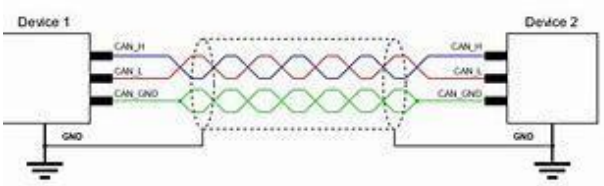

Fig.2 CAN BUS Wiring and Transmission

The Controller Area Network (CAN) bus protocol finds extensive applications across various industries due to its reliability, efficiency, and versatility. In automotive systems, CAN bus serves as the backbone for communication among electronic control units (ECUs) within vehicles, enabling functionalities such as engine management, transmission control, anti-lock braking systems (ABS), airbag deployment, and vehicle diagnostics. It allows different subsystems to exchange information in real-time, enhancing vehicle performance, safety, and fuel efficiency. Beyond automotive, CAN bus is widely utilized in industrial automation and control systems. It enables communication between sensors, actuators, programmable logic controllers (PLCs), and other devices in manufacturing plants, facilitating tasks such as process monitoring, machine control, and inventory management. CAN bus's deterministic nature ensures timely transmission of data critical for maintaining operational efficiency and safety in industrial environment. Moreover, CAN bus is employed in various other domains such as aerospace, maritime, medical devices, and consumer electronics. In aerospace and maritime applications, it supports avionics and navigation systems, while in medical devices, it enables communication between sensors, monitors, and control units in equipment like patient monitors and diagnostic machines. Additionally, CAN bus is utilized in consumer electronics for home automation, gaming peripherals, and multimedia systems, providing a standardized communication interface for connecting different devices seamlessly.

The flexibility, reliability, and cost-effectiveness of CAN bus make it a preferred choice in applications where real-time communication, robustness, and interoperability are paramount. Its wide-ranging adoption across diverse industries underscores its significance as a fundamental communication protocol driving innovation and efficiency in modern technological systems.

III PROPOSED METHOD

LoCoCAT for Electronic Control Units (ECUs) in vehicles is a cutting-edge application of location-based technology tailored specifically for automotive systems. This innovative platform offers a range of features designed to enhance vehicle performance, safety, and efficiency. Its core functionality includes real-time location tracking of vehicles, enabling fleet managers to monitor the precise whereabouts of their assets at any given moment. Additionally, LoCoCAT integrates geofencing capabilities, allowing for the creation of virtual boundaries around specific areas. This feature enables proactive management of vehicle movement and facilitates automatic notifications when vehicles enter or exit predefined zones, thereby improving security and enabling more efficient routing. Furthermore, LoCoCAT provides diagnostic data from onboard ECUs, offering insights into vehicle health and performance metrics. By leveraging this data, automotive professionals can proactively address maintenance issues, optimize fuel consumption, and prolong the lifespan of vehicle components. Overall, LoCoCAT for ECUs in vehicles empowers fleet operators and automotive manufacturers with actionable insights, streamlined operations, and enhanced safety measures, ultimately leading to improved productivity, cost savings, and customer satisfaction.

LoCoCAT for Electronic Control Units (ECUs) in vehicles offers a comprehensive suite of features tailored to optimize vehicle management and performance. Its core functionalities include real-time location tracking, allowing for precise monitoring of vehicle whereabouts. Geofencing capabilities enable the creation of virtual boundaries, facilitating proactive management of vehicle movement and enhancing security. Additionally, LoCoCAT provides diagnostic data from onboard ECUs, offering valuable insights into vehicle health and performance metrics. This data empowers automotive

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.3, August : 2024

professionals to proactively address maintenance issues, optimize fuel consumption, and extend the lifespan of vehicle components. Moreover, LoCoCAT offers seamless integration with existing vehicle systems, ensuring compatibility and ease of implementation. Overall, the diverse features of LoCoCAT contribute to improved operational efficiency, enhanced safety measures, and greater cost-effectiveness in vehicle management.

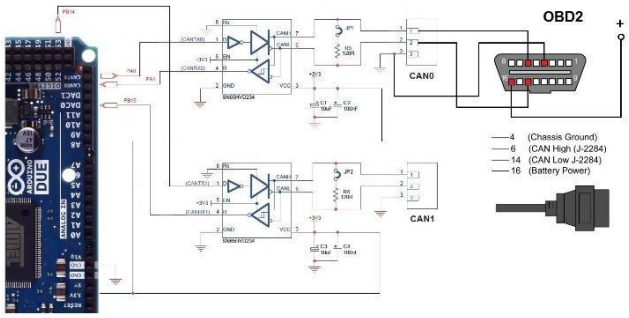

Fig.3 Threats faced by the ECU's in the Electric Vehicles

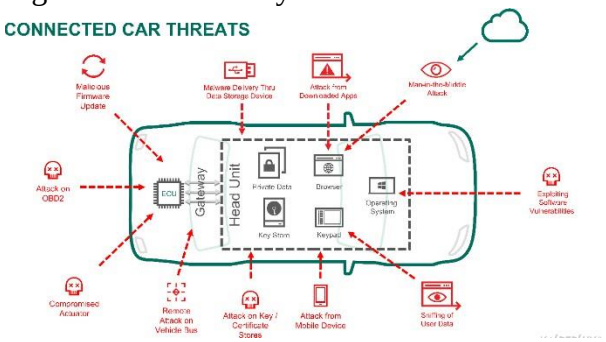

Fig.4 Circuit Diagram of Arduino Due interfacing with CAN Transreceiver .

The operational sequence empowers the users to see the working of the sensors interfaced with the ECU, leading to the continuous monitoring of the vehicle's condition and message encryption.The accuracy of LOCoCAT's classification hinges on several critical factors. First and foremost, the quality and diversity of the training data play a pivotal role. A meticulously labeled dataset encompassing a broad spectrum of attack scenarios greatly enhances LOCoCAT's accuracy. Equally vital is the process of feature extraction and selection from the corrupted CAN bus data, as the relevance and effectiveness of these features directly impact the model's accuracy. Additionally, the choice of machine learning model—be it decision trees, random forests, or neural networks—significantly influences the accuracy, with certain models outperforming others for specific attack types. Beyond mere accuracy, evaluation metrics such as precision, recall, and F1-score offer a more nuanced understanding of LOCoCAT's performance, accounting for factors like false positives and false negatives. Furthermore, the inherent challenges of CAN bus attacks, including their subtlety and context-dependency, coupled with real-world complexities and variations in network conditions, pose significant hurdles to accurate classification. To validate LOCoCAT's accuracy, researchers typically benchmark it against existing methods and datasets, underscoring the importance of thorough evaluation and contextual interpretation within the domain of CAN bus security.

IV. DESIGN OF WORKING MODEL

In this setup, Arduino Due is to connected to a CAN controller (such as the MCP2515) and a CAN transceiver (like the SN65HVD230). Connect the 3.3V pin of the SN65HVD230 to the 3.3V pin of the Arduino Due. Connect the GND pin of the SN65HVD230 to the GND pin of the Arduino Due. Connect the TX (transmit) pin of the SN65HVD230 to a digital pin (e.g., Pin 0) on the Arduino Due. Connect the RX (receive) pin of the SN65HVD230 to another digital pin (e.g., Pin 1) on the Arduino Due. Connect it to the CAN bus using the appropriate connectors (usually DB9 or OBD-II). Power it up and configure it to listen to the CAN bus traffic.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 8, No.3, August : 2024

V. RESULT ANALYSIS

The result analysis of CANVAST identifies different types of attacks on the CAN bus, including: Bus Flood Attack which is flooding the bus with a large number of messages to overwhelm its capacity. Simple Frame Spoofing is sending forged messages to deceive other ECUs. Adaptive Spoofing is dynamically adjusting the spoofed messages to avoid detection. Error Passive Spoofing Attack is exploiting error handling mechanisms to inject malicious messages. Double Receive Attack is the manipulation of the bus arbitration process to gain control. Bus- Off Attack is forcing an ECU into a bus-off state by exceeding error limits. Freeze Doom Loop Attack: Causing a loop of freeze frames that disrupt communication. To mitigate these attacks, intrusion detection systems (IDS) play a crucial role. The result analysis emphasizes the importance of real-time traffic analysis and payload analysis within IDS.

A. CANVAST and LoCoCAT Technology

This project works on two technologies: CANVAST and LOCoCAT where CANVAST focuses on analysing the security vulnerabilities of the Controller Area Network (CAN), which is commonly used in automotive systems. It investigates various types of attacks on the CAN bus and emphasizes the importance of intrusion detection systems (IDS) for safeguarding against these threats. LOCOCAT (Localizing Cyber-Physical Attacks in Automotive Systems) is another initiative related to automotive cybersecurity which aims to develop techniques for localizing cyber-physical attacks within the vehicle's network, enabling better response and mitigation strategies.

B. Output Analysis

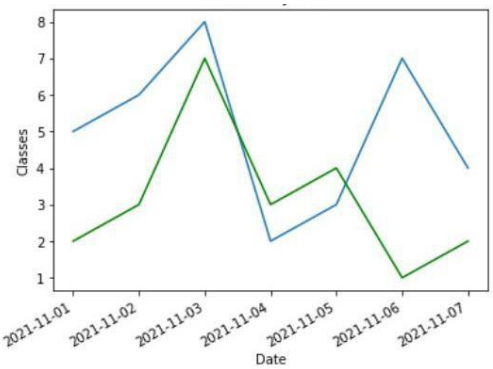

Fig 5 Graph between Time and Data received from the Sensors

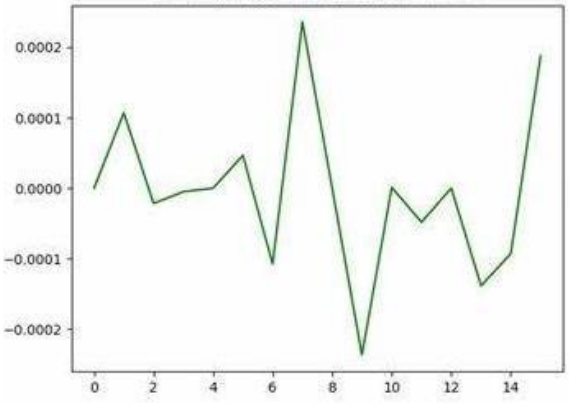

Fig.6 The Output of Data Vulnerability in Electric Vehicle

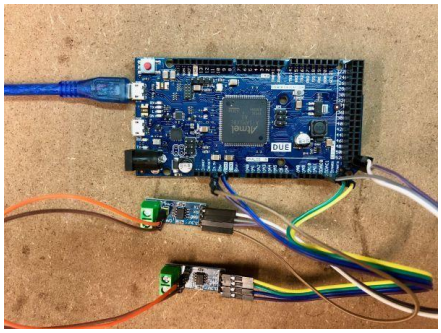

Fig.7 Hardware Setup of CANVAST: CAN BUS Security Analysis

LOCoCAT is designed to minimize resource usage while achieving accurate intrusion detection. It adds minimal computational overhead, making it suitable for real-time applications. By efficiently classifying attacks, LOCoCAT ensures timely responses without compromising system performance and achieves high accuracy within the first 50 milliseconds of an attack.

VI. CONCLUSION

The CAN Bus Security Analysis evaluates two significant frameworks, LoCoCAT and CANVAST, shedding light on crucial aspects of CAN bus security. LoCoCAT introduces a novel method for efficiently classifying intrusions by grouping messages, extracting pertinent features, and employing a lightweight classifier model, thus mitigating computational overhead while effectively identifying and categorizing CAN bus attacks. On the other hand, CANVAST provides a comprehensive examination of CAN bus security challenges, emphasizing the necessity of safeguarding the bus against potential vulnerabilities and risks. It elucidates various access points to the CAN bus and outlines a spectrum of attacks ranging from bus floods to spoofing and bus-off attacks. The analysis underscores the importance of intrusion detection systems for real-time monitoring and payload analysis and advocates for the implementation of CAN security gateways with firewalling functions to ensure robust protection of the CAN bus.

FUTURE WORK

In the realm of CAN bus security, several avenues for future exploration and improvement emerge. Enhanced Intrusion Detection Systems (IDS) present a promising area, with potential advancements in tailored algorithms and the integration of machine learning techniques like deep learning for more accurate anomaly detection. Secure Key Management stands out as critical for securing communication on the CAN bus, urging research into cryptographic solutions and secure key exchange protocols to thwart unauthorized access. Behavioral Profiling offers another avenue, advocating for the creation of profiles based on CAN bus traffic to detect anomalies indicative of attacks. Secure CAN Bus Gateways are also crucial, necessitating the development of robust security gateways with filtering capabilities and secure communication channels with Electronic Control Units (ECUs). Additionally, exploring Physical Layer Security mechanisms, standardization efforts, redundancy strategies, and security awareness training are essential to fortifying the resilience of CAN bus networks against potential threats. These areas collectively represent a comprehensive roadmap for advancing CAN bus security in the automotive domain.

REFERENCES

[1] H. Ko, T. Kim, D. Jung and S. Pack, "Software-Defined Electric Vehicle (EV)-to-EV Charging Framework with Mobile Aggregator," in IEEE Systems Journal, vol. 17, no. 2, pp. 2815- 2823, June 2023, doi: 10.1109/JSYST.2023.3240509.

[2] D. Mishra, B. Singh and B. K. Panigrahi, "Bi-Directional EV Charging with Robust Power Controlled Adaptive Phase-Shift Algorithm," in IEEE Transactions on Vehicular Technology, vol. 72,

no. 12, pp. 15491-15501, Dec. 2023, doi: 10.1109/TVT.2023.3290116.

[3] C. Sun, R. Wang, Q. Sun and H. Zhang, "A Novel Synchronous Rectification Scheme with Low Computational Burden for LLC Resonant Converter in EV Charger Applications," in IEEE Transactions on Industrial Electronics, vol. 70, no. 9, pp. 8991- 9003, Sept. 2023, doi: 10.1109/TIE.2022.3215445.

[4] N. Patel, L. A. C. Lopes, A. Rathore and V. Khadkikar, "A Soft- Switched Single-Stage Single-Phase PFC Converter for Bidirectional Plug-In EV Charger," in IEEE Transactions on Industry Applications, vol. 59, no. 4, pp. 5123-5135, July-Aug.
2023, doi: 10.1109/TIA.2023.3270387.

[5] J. Ye et al., "Cyber–Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges, and Future Visions," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 4, pp. 4639-4657, Aug. 2021, doi: 10.1109/JESTPE.2020.3045667.

[6] M. Ali, G. Kaddoum, W. -T. Li, C. Yuen, M. Tariq and H. V. Poor, "A Smart Digital Twin Enabled Security Framework for Vehicle-to-Grid Cyber-Physical Systems," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5258-5271, 2023, doi: 10.1109/TIFS.2023.3305916.

[7] Z. Pourmirza and S. Walker, "Electric Vehicle Charging Station: Cyber Security Challenges and Perspective," 2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada, 2021, pp. 111-116, doi: 10.1109/SEGE52446.2021.9535052.

[8] K. Halba, E. Griffor, P. Kamongi and T. Roth, "Using Statistical Methods and Co-Simulation to Evaluate ADS-Equipped Vehicle Trustworthiness," 2019 Electric Vehicles International Conference (EV), Bucharest, Romania, 2019, pp. 1-5, doi: 10.1109/EV.2019.8892870.

[9] A. Almarshoodi, J. Keenan, I. Campbell, T. Hassan, M. I. Ibrahem and M. M. Fouda, "Security and Privacy Preservation for Future Vehicular Transportation Systems: A Survey," 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 2023, pp. 728- 734, doi: 10.1109/CSNT57126.2023.10134677.

[10] J. Kandasamy, S. Arunagirinathan, P. Sivaraj, M. Pameela, G. T. Subham and R. Nagarajan, "Detection of Cyber Attack in Electric Vehicles using ALSTM based Machine Learning," 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2022, pp. 596-600, doi: 10.1109/ICIRCA54612.2022.9985609.