A Model for Identifying and Isolating Sensor Attacks in Autonomous Vehicles

P.Haritha[1], P. Punitha[2], Ch. Niranjan Kumar[3] and Deepa Panse[4]

[1] Department of CSE, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India
patti.haritha@gmail.com
[2] Department of CSE(DS), Vignana Bharathi Institute of Technology, Hyderabad, Telangana, India
[3] Department of CSE, CVR College of Engineering, Hyderabad, Telangana, India
[4] Department of CSE, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India

Abstract. The proposed solution in this paper is model-based which aims to address the cyber-security threats affecting automated cars more so those affecting the sensors-targets. The goal of the framework is to detect the risks and find their position to provide secure positioning of the AVs. To build a tenacious protection against cyber threats the technique involves having multiple sensors to incorporate many physical sensors that give real time posture. For real-time detection of anomalies in the sensor measurements the design involves an extended Kalman filter (EKF) and a cumulative sum (CUSUM) discriminator. Iterator calculations of the position and orientation of a vehicle are carried out using Extended Kalman Filters (EKFs). At the same time, there are CUSUM discriminators employed in evaluating the differences between actual and expected positions in line with the vehicle mathematical model or failure identification. An auxiliary detector combines the information from several sensors to evaluate disparities in measurements. The results obtained from all the detectors are used to develop a rule-based isolation method that accurately identifies the source of the abnormal sensor. The effectiveness of the proposed architecture is further described by incorporating actual vehicle data, which also stress on helping protect autonomous vehicles from cyber risks.

1.INTRODUCTION

In the last couple of years, the development of autonomous driving technologies has launched an epoch of innovative age in transportation with driverless cars being already tested on public roads. For self-driving car frame, it uses several sensors like GPS, LiDAR, Camera in order to recognize its own position, and to discern the environment for smart transportation system. These sensors also make self-driven cars more vulnerable to cyber-crimes, it forms a major challenge to the reliable operation of self-driven cars.

The possibilities of this kind of attack to the self-driving cars are as follows, both of first order disruption and second order disaster. Many studies have proved that such an attack is possible other studies also showed that such attacks are possible. GPS spoofing is the manipulation of GPS signals; cars may deviate from the intended route [2].

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

LiDAR spoofing attacks can manipulate point clouds in two ways: disregarding real-life barriers or inventing fake ones in front of the car [3]. This is especially true for the optical flow sensors, which have been found to be vulnerable to spoofing that messes up the car's motion perception [4]. Also, often-used robotics middleware like the Robot Operating System (ROS) multiplies the risk since it makes it easier to manipulate sensor data [5]. Because of these risks, shielding self-driving vehicles from real-time sensor attacks have become one of the most important challenges in the study of cybersecurity.

This paper focuses on the emerging need for methods to detect and identify cyber-attacks targeting the localisation sensors of self-driving cars such as GPS and LiDAR which are core parts of the navigation systems. In the pre-said decade, threats and risks associated with cyber-security of self-driving cars have been on focus of numerous researchers especially for the last five years. Substantial findings involve investigations regarding possible cyber-attacks on self-driving cars and recommendations on such threats. Furthermore, the categorisation of attack types and countermeasures for them has been advanced in order to gain a better understanding of autonomous vehicle cybersecurity [7].

The strategies to address cyber-security issues in autonomous vehicles can be roughly categorised into two main types: There are two types of MIS: information-oriented and control-oriented. As for the information centric approaches, the methodologies put emphasis on the protection means such as encodings and user login to enhance the security of the systems of autonomous vehicles [8-13]. These strategies may work well against external threats; however, internal adversaries familiar with cryptographic systems and the capability to manipulate onboard components may not be effectively countered as well.

On the other hand, control-based approaches analyse the kinematics of the cyber-attacks and impact on the vehicle's control system [14]. These methodologies improve security steps to determine the consequences arising from attack systems through modeling, which provides greater security than information-based methods and improves the ability of automobile systems to resist malicious cyber threats.

Control-oriented techniques can be categorised into two main classes: data-driven and model-based. Analysed approaches rely on machine learning algorithms to define anomalies by comparing the last measurements with previous values [16 - 21]. However, such systems present several drawbacks arising from their use of training data sets, and potential problems may arise when the systems fail to recognize fundamentally new or less well-known threats.

On the other hand, model-based methodologies have detected deviations in the actual value of the sensed variables from the expected behaviour predicted on the basis of the mathematical model of the vehicle [22 - 25]. While in theory model-based detectors can be very efficient, in practice they may not discover stealthy attacks hidden under the veil of uncertainty.

The central goal of this research is to enhance the cyber security of autonomous vehicles through the development of new techniques for online detection and source identification of sensor attacks. Our goal is to improve the autonomous vehicle systems against new types of cyber threats using the information and control theories paradigms collectively to ensure the safety of the systems and their reliability to operate on the roads safely.

2.LITERATURE SURVEY

The area of self-driving cars is relatively new, and therefore, significant research has been conducted on its security since it is vulnerable to malicious attacks. The identified literature reveals a rather ambiguous body of studies aimed not only at understanding but also at recognizing and combating cyber threats targeting self-driving vehicles.

Kerns et al [1] present a core investigation examining vulnerability of unmanned aircraft to GPS spoofing attacks. The authors provide a clear example of the possibility to capture and lead UAVS by interfering with GPS-signals, this illustrates the need for robust countermeasures against such threats. This work is basic to understanding the possible implications of cyber-attack on autonomous systems.

David et al [3] look at the domain of unmanned aerial vehicles (UAVs) through analyzing sensor input spoofing attacks. By changing the inputs from the sensors, the enemies are able to manipulate the UAVs creating major dangers to their operations and existence. This work also reveals the importance of preventing sensor data tampering due to the impact of cyber threats to self-driving cars.

Hence, from a broader perspective of autonomous cars, Petit and Shladover [5] analyses cyber-vulnerabilities and their impacts. The authors point out numerous attack scenarios and demonstrate that GPS spoofing and wireless communication vulnerability exist which makes it critically important to enhance security in the systems of autonomous vehicles. The present work sets the starting point for researching how automated cars are tender towards the cyber-security problems.

Parkinson et al. [7] provide extensive discussion on cyber threats that are facing self- and smart; they raise future challenges and countermeasures in this area. The authors explain various types of threats in the context of evolving cyber risks in the automotive industry through the discussion of specific attack techniques and the resulting impact on the vehicle's functionality. This paper is a useful reference for understanding the vast spectrum of cyber threats in self- and Internet-connected cars.

Suo and Sarma.[11] propose real-time trust enhancement techniques that can counter the acts in connected and automated vehicles. Specifically, the authors aim at enhancing the protection against cyber threat on the automated automobile through the use of trust-based methodologies. Thus, this paper outlines approaches towards the improved cybersecurity of connected vehicle systems and encourages subsequent research on trust-based defence mechanisms.

To emphasize, Van Wyk et al. [17] focused on real-time methods for identifying sensors' anomalies in automated vehicles. To minimize the impact of the primary threats such as sensor spoofing assaults to vehicle operation, the authors seek to build complex detection strategies. The strength of this work is the extension of the current scientific knowledge on the recognition and eradication of cyber risks to AV systems that offers immediate advice for managing threats in real time.

Keipour et al. [25] call for a real-time automated abnormality detection process in autonomous UAVs while employing machine learning techniques to identify strange behaviors. The authors want to propose complex sensor data analysis for real-timing detection of cyber-attacks on aerial vehicles for their secure and reliable operation in hostile environment. This study highlights the importance of adaptive defence mechanism in combating new generation cybers threats.

Rajbahadur et al. [26] discussed a detail review of the anomaly detection techniques for cybersecurity and safety in connected vehicles. Through analyzing different approaches, the authors enlighten the community on the existing progress in anomaly detection as well as the strategies used in its mitigation. This survey is quite valuable for

the researcher or practitioner who wants to address the cyber-security issues in connected car systems.

The literature review establishes that the cyber-security risk faced by autonomous vehicles is rather diverse and numerous. Many works have been done by researchers to detect and analyze various attack strategies such as GPS spoofing and modification of the sensor input signals and several defense methods have also been proposed. To overcome these difficulties, a multilevel approach is required creating enhanced detection algorithms, continuous monitoring platforms, and robust trust management for protecting the AV systems from progressively developing cyber threats.

3.1 METHODOLOGY

3.1.1 Proposed Work

This lesson offers a detailed approach for systematically processing online data acquired from GPS and LiDAR sensors with consideration of three attack detecting mechanisms. Each detector uses an Extended Kalman Filter (EKF) for the pose evaluation together with a Cumulative Sum (CUSUM) discriminator. The first two detectors make independent estimations of the car's pose estimate based on GPS data along with LiDAR data and continuously track deviations from the expected state. The third detector incorporates a fusion process of two signal measurements to determine their reliability and in the process enhance the detection capacity. Despite the fact that they employ different sensor fusion methodologies, all detectors abide by the same principles where the use of Statistics EKF for estimating and CUSUM for detecting potentially malicious accounts for sensor attacks to ensure safe localization of autonomous cars.

3.1.2 System Architecture

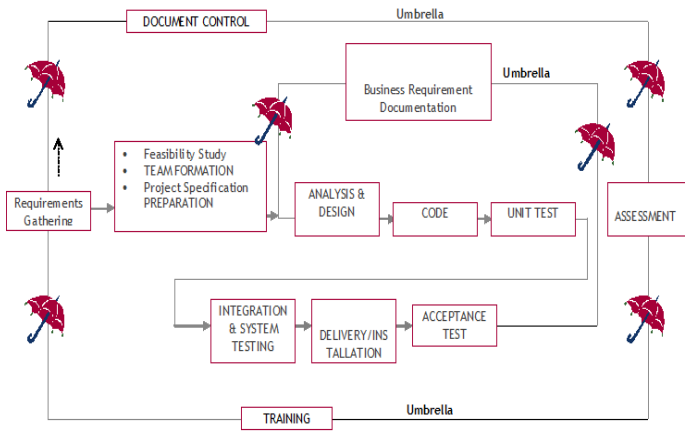

Fig. 1: Proposed Architecture

Document control, evaluation and training, and requirement collection system architecture has several components linked with each other. The design must afford seamless inter and intra functional communication and information sharing. It begins with assessment of project viability and creation of a team, followed by formulation of a project charter and developing of the system's use cases. The analysis and design steps map these requirements into system parts and contexts. This involves the creation of

applications, independent testing of small modules and linking of the modules to form a large system. System testing ensures reliability or the ability of a system to perform well and meet user requirements. The delivery and installation phases bring the start to the system operation; after which, acceptance testing to ascertain user requirements conformity. In the architecture effective data management, rather high security requirements and user-friendly interfaces always play a crucial role in the development of the system. There is a need to ensure that it is scalable and adaptable in future for expansion or when fulfilling new demands. The design aims at enhancing the effectiveness of the functioning, stability of work, and availability of secure environment for document handling, assessment, training, and exercising requirements management.

3.1.3 Upload GPS Dataset

This module allows users to effectively upload GPS data into the application. This feature also allows one to integrate GPS data and then transition the data into the system for further analysis and manipulation. He/she can then choose the GPS dataset of their preference, then follow through with the upload and in essence help to enhance the input of data and aid the incorporation of GPS data for various studies throughout the system.

3.1.4 Upload LiDAR Dataset

This module allows users to easily feed LiDAR datasets into the program, thus enlarging LiDAR data for analysis and computation. The module enhances data management functionality within the application; as it enables easy incorporation of LiDAR data hence enabling the use of LiDAR measurements in different analysis and algorithms. It provides users with the needed attributes for effective operation in handling LiDAR data for navigation and detection leading to enhanced productivity in the use of such vehicles and related projects.

3.1.5 Run GPS Extended Kalman Filter

This module employs the GPS Extended Kalman Filter method for anticipations of vehicle positions using raw GPS data. Using imprecise GPS measurements, the Kalman filter allows the system to estimate an exact position and orientation of the vehicle. The filter refines its predictions by updating it with current sensor data as well as the dynamic model of the system in real-time sequences. This approach also enables the generation of better and reliable state estimates of the vehicle, which improves the precise localization in complex environments. The GPS Extended Kalman Filter enhances the level of reliability and accuracy of vehicle tracking with GPS data.

3.1.6 Run LIDAR Extended Kalman Filter

In this module, raw LiDAR data is predicted to vehicle positions using the LiDAR Extended Kalman Filter algorithm. The Kalman filter is used to forecast the position and orientation of the vehicle by using the LiDAR unprocessed data. The filter continues to improve its estimates by combining current sensor information with the dynamic model of the vehicle using a recursive process. This iterative approach enhances the accuracy and the reliability as well in vehicle localization and is thus suitable in areas that are constantly changing such as roads

.

3.1.7 Run Rule Based CUSUM Detector

It also runs a Rule-Based Cumulative Sum (CUSUM) Detector to analyze data from the Extended Kalman Filter (EKF). Based on the CUSUM analysis on EKF data, the system indicates significant departures from expected values. In case of detection of major disturbance, the module sets an alarm, indicating a probable violation of a sensor. It helps enhance the robustness of the system to sensor data outliers by making it easier to identify and contain adversarial threats to the safety and security of self-driving vehicles.

3.1.8 Attack Detection Graph

The last component of the system is the Attack Detection Graph that provides a graphical representation of the total attacks detected by LiDAR and GPS sensors. This module also enables users to observe the frequency and distribution of the detected assaults over time in order to evaluate the operation of the sensor-based attack detection system. To this end, a dynamic plotting of the attack data empowers the user to analyze the effectiveness of a particular detection technique while also determining the general security status of the autonomous vehicle system

4.EXPERIMENTAL RESULTS

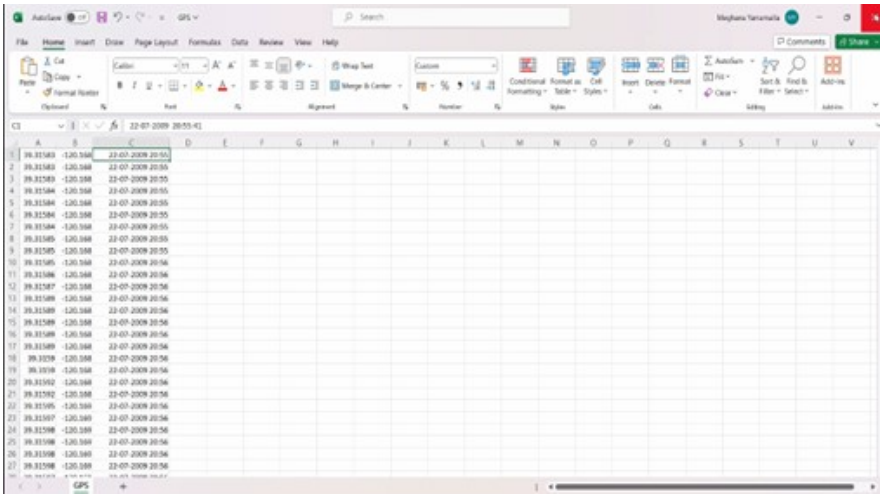

Fig. 2: 132 rows – GPS.CSV

Figure 2 shows GPS data recorded by the latitude and longitude values of the car's location with date and time stamps. The data set has 132 rows for the identification of vehicle sensor attacks.

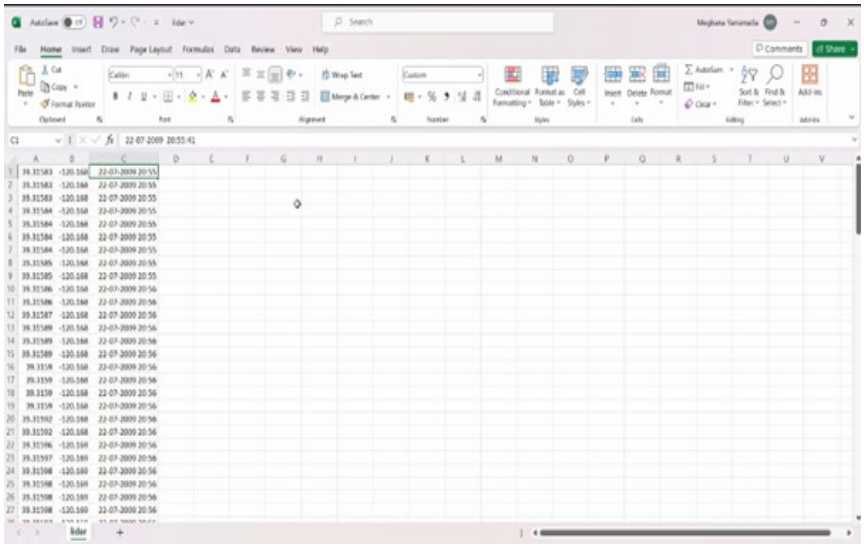

Fig. 3: 132 rows – LIDAR.CSV

A LIDAR dataset that contains the latitude and longitude coordinates of the vehicle along with date and time has been depicted in the Figure 3. The dataset has 132 rows of data to detect sensor attacks on the vehicle. Upon executing the project, a screen appears presenting choices to upload the datasets. We must submit both GPS and LIDAR datasets according to the settings available on the output screen.

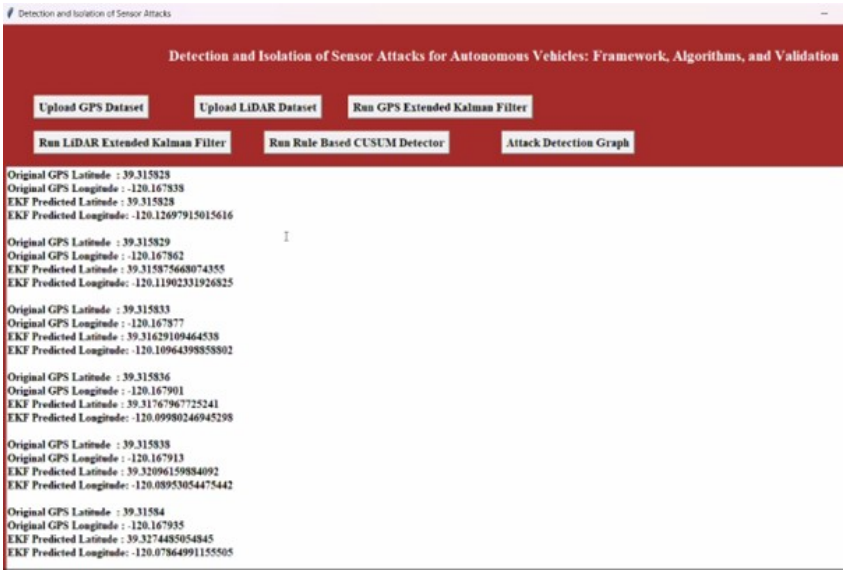

Fig. 3: GPS Extended Kalman filter

After uploading the datasets, run the GPS extended Kalman filter. It shows the original and predicted values of latitude and longitude as shown in fig3.

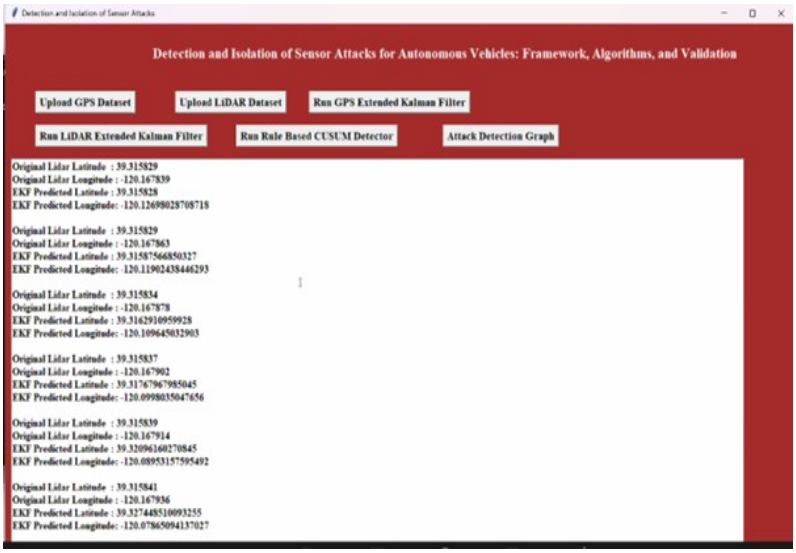

Fig. 4: LIDAR Extended Kalman filter

After running the GPS EKF, ‘run LIDAR Extended Kalman filter’. It shows the original and predicted values of latitude and longitude as show in fig4. we can see there is narrow difference between original and predicted values.

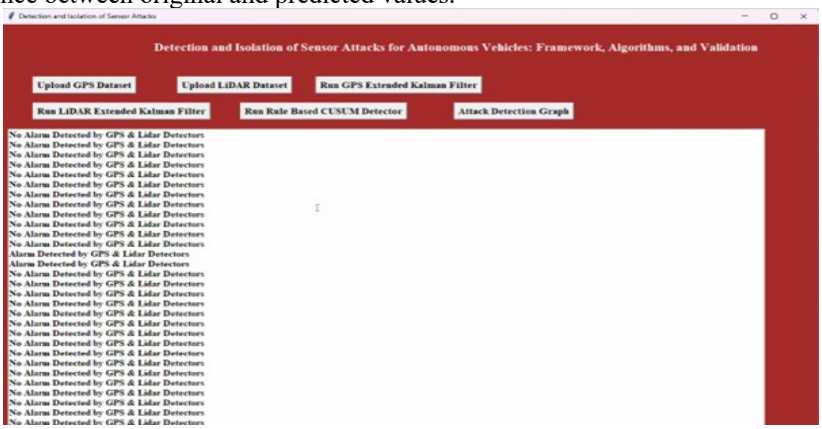

Fig. 5: Rule based CUSUM detector

Now ‘Run Rule Based CUSUM Detector’ to find variations between original and predicted values and for each latitude and longitude CUSUM has applied rules to detect attack and in fig5 we can see GPS and LIDAR attack detected and in other records NO ALARM DETECTED. You can scroll down the screen to view all detections.

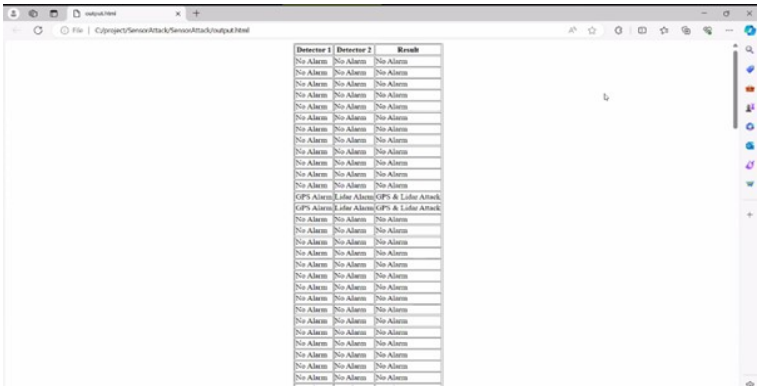

Fig. 6: Attack detection output

Now click on 'Attack Detection Graph' to get the output result. In above fig6, we can see alarm and no alarm for both detectors. We get the alarm when there is a huge difference between the original and predicted values of lattitude and longitude. The alarm specifies the sensor attack of the vehicle.

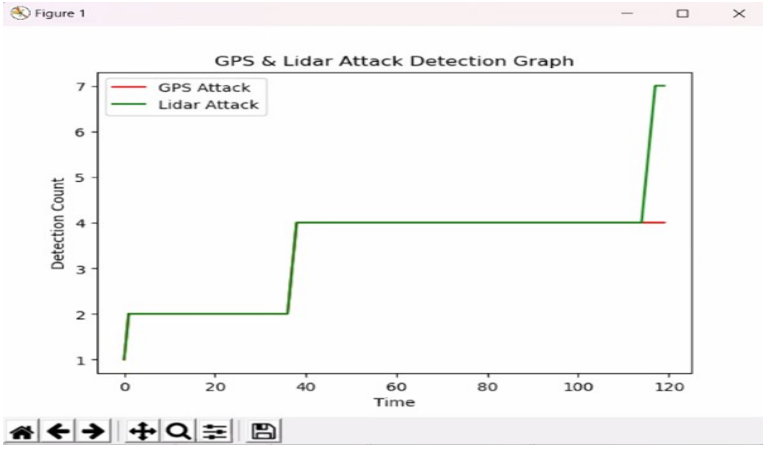

Fig. 7: Attack detection graph

In above graph, x-axis represents TIME and y-axis represents attack detection count and red line represents GPS attack and green line represents Lidar attack and in above graph we can see GPS (detector 1) detected total 4 attacks from 0 to 120 records and lidar (detector 2) detected 7 attacks.

5.CONCLUSIONS

This research presents a robust model-based architecture designed to detect and isolate cyber-attacks targeting sensors in autonomous vehicles. The system utilizes a collection of attack detectors and a rule-based isolation method to recognize sensor attacks and ascertain their sources, significantly enhancing the cybersecurity of autonomous vehicles. The efficacy of the proposed design is evidenced by experimental validation using actual vehicle data. The trials encompassed four common types of assaults: Denial of Service (DoS), False Data Injection (FDI), stealth attacks, and replay attacks. These categories were employed to construct seven distinct attack scenarios.

The effective identification of GPS stealthy attacks is particularly significant, as these attacks represent a very advanced form that can elude detection by conventional model-based methods. This achievement underscores the effectiveness of the auxiliary detector, which identifies inconsistencies among various sensor data, hence enhancing the system's resilience against covert attacks.

6.FUTURE SCOPE

Future research opportunities arise from this study on improving cyber-security in autonomous vehicles. Initially, investigating advanced machine learning methodologies, particularly deep learning, may enhance the framework's detection capabilities by allowing the system to autonomously learn and adapt to changing attack plans.
Furthermore, incorporating anomaly detection algorithms that consider contextual information and environmental variables could improve the system's capacity to differentiate between legitimate anomalies and hostile intrusions, hence minimizing false positives and augmenting overall detection precision.

Moreover, broadening the framework's breadth to encompass future vulnerabilities, such as adversarial assaults on machine learning models utilized in autonomous vehicles, will be essential. This entails establishing strong safeguards against advanced assaults targeting sensor inputs and influencing decision-making procedures.

7.REFERENCES

1. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, “Unmanned aircraft capture and control via GPS spoofing,” J. Field Robot., vol. 31, no. 4, pp. 617–636, Jul. 2014.
2. Y. Cao et al., “Adversarial sensor attack on LiDAR-based perception in autonomous driving,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Nov. 2019, pp. 2267–2281.
3. D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, “Controlling UAVs with sensor input spoofing attacks,” in Proc. 10th USENIX Workshop Offensive Technol. (WOOT), 2016, pp. 221–231.
4. N. DeMarinis, S. Tellex, V. P. Kemerlis, G. Konidaris, and R. Fonseca, “Scanning the Internet for ROS: A view of security in robotics research,” in Proc. Int. Conf. Robot. Autom. (ICRA), May 2019, pp. 8514–8521.
5. J. Petit and S. E. Shladover, “Potential cyberattacks on automated vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546–556, Apr. 2015.
6. V. L. L. Thing and J. Wu, “Autonomous vehicle security: A taxonomy of attacks and defences,” in Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData), Dec. 2016, pp. 164–170.
7. S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber threats facing autonomous and connected vehicles: Future challenges,” IEEE Trans. Intell. Transp. Syst., vol. 18, no. 11, pp. 2898–2915, Nov. 2017.
8. Bezemskij, G. Loukas, R. J. Anthony, and D. Gan, “Behaviour based anomaly detection of cyber-physical attacks on a robotic vehicle,” in Proc. 15th Int. Conf. Ubiquitous Comput. Commun. Int. Symp. Cyberspace Secur. (IUCC-CSS), Dec. 2016, pp. 61–68.
9. Bezemskij, G. Loukas, D. Gan, and R. J. Anthony, “Detecting cyber physical threats in an autonomous robotic vehicle using Bayesian networks,” in Proc. IEEE Int. Conf.

Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData), Jun. 2017, pp. 98–103.
10. M. Olivato, O. Cotugno, L. Brigato, D. Bloisi, A. Farinelli, and L. Iocchi, "A comparative analysis on the use of autoencoders for robot security anomaly detection," in Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS), Nov. 2019, pp. 984–989.
11. D. Suo and S. E. Sarma, "Real-time trust-building schemes for mitigating malicious behaviors in connected and automated vehicles," in Proc. IEEE Intell. Transp. Syst. Conf. (ITSC), Oct. 2019, pp. 1142–1149.
12. F. Jiang, B. Qi, T. Wu, K. Zhu, and L. Zhang, "CPSS: CP-ABE based platoon secure sensing scheme against cyber-attacks," in Proc. IEEE Intell. Transp. Syst. Conf. (ITSC), Oct. 2019, pp. 3218–3223.
13. R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle," IEEE Access, vol. 7, pp. 138018–138031, 2019.
14. C. Kwon, W. Liu, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks," in Proc. Amer. Control Conf., Jun. 2013, pp. 3344–3349.
15. H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo, "Bibliographical review on cyber attacks from a control oriented perspective," Annu. Rev. Control, vol. 48, pp. 103–128, 2019.
16. Á. M. Guerrero-Higueras, N. DeCastro-García, and V. Matellán, "Detection of cyber-attacks to indoor real time localization systems for autonomous robots," Robot. Auto. Syst., vol. 99, pp. 75–83, Jan. 2018.
17. F. van Wyk, Y. Wang, A. Khojandi, and N. Masoud, "Real-time sensor anomaly detection and identification in automated vehicles," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 3, pp. 1264–1276, Mar. 2020.
18. Ferdowsi, U. Challita, W. Saad, and N. B. Mandayam, "Robust deep reinforcement learning for security and safety in autonomous vehicle systems," in Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC), Nov. 2018, pp. 307–312.
19. Rasheed, F. Hu, and L. Zhang, "Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN," Veh. Commun., vol. 26, Dec. 2020, Art. no. 100266.
20. N. Patel, A. Nandini Saridena, A. Choromanska, P. Krishnamurthy, and F. Khorrami, "Adversarial learning-based on-line anomaly monitoring for assured autonomy," in Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS), Oct. 2018, pp. 6149–6154.
21. Y. Wang, N. Masoud, and A. Khojandi, "Real-time sensor anomaly detection and recovery in connected automated vehicle sensors," IEEE Trans. Intell. Transp. Syst., vol. 22, no. 3, pp. 1411–1421, Mar. 2021.
22. Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 12, pp. 3893–3902, Dec. 2018.
23. E. Mousavinejad, F. Yang, Q.-L. Han, X. Ge, and L. Vlacic, "Distributed cyber attacks detection and recovery mechanism for vehicle platooning," IEEE Trans. Intell. Transp. Syst., vol. 21, no. 9, pp. 3821–3834, Sep. 2020.
24. G. Sabaliauskaite, G. S. Ng, J. Ruths, and A. Mathur, "A comprehensive approach, and a case study, for conducting attack detection experiments in cyber–physical systems," Robot. Auton. Syst., vol. 98, pp. 174–191, Dec. 2017.
25. Keipour, M. Mousaei, and S. Scherer, "Automatic real-time anomaly detection for autonomous aerial vehicles," in Proc. Int. Conf. Robot. Autom. (ICRA), May 2019, pp. 5679–5685.

26. G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, “A survey of anomaly detection for connected vehicle cybersecurity and safety,” in Proc. IEEE Intell. Vehicles Symp. (IV), Jun. 2018, pp. 421–426.
27. The Autoware Foundation–Open Source for Autonomous Driving. Accessed: Mar. 9, 2020.
28. J. Giraldo et al., “A survey of physics-based attack detection in cyberphysical systems,” ACM Comput. Surv., vol. 51, no. 4, pp. 1–36, 2018.
29. Sadaf, Memoona, et al. "A Novel Framework for Detection and Prevention of Denial of Service Attacks on Autonomous Vehicles using Fuzzy Logic." *Vehicular Communications* (2024): 100741.
30. Micale, Davide, et al. "A context-aware on-board intrusion detection system for smart vehicles." *International Journal of Information Security* (2024): 1-21.
31. M. Begum, G. Raja and M. Guizani, "AI-based Sensor Attack Detection and Classification for Autonomous Vehicles in 6G-V2X Environment," in IEEE Transactions on Vehicular Technology, doi: 10.1109/TVT.2023.3334257.
32. P. Mansourian, N. Zhang, A. Jaekel and M. Kneppers, "Deep Learning-Based Anomaly Detection for Connected Autonomous Vehicles Using Spatiotemporal Information," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 12, pp. 16006-16017, Dec. 2023, doi: 10.1109/TITS.2023.3286611.
33. S. Baccari, M. Hadded, H. Ghazzai, H. Touati and M. Elhadef, "Anomaly Detection in Connected and Autonomous Vehicles: A Survey, Analysis, and Research Challenges," in IEEE Access, vol. 12, pp. 19250-19276, 2024, doi: 10.1109/ACCESS.2024.3361829.
34. S. Yan, Z. Gu, J. H. Park and M. Shen, "Fusion-Based Event-Triggered State Estimation of Networked Autonomous Surface Vehicles With Measurement Outliers and Cyber-Attacks," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2024.3350536.
35. Devi, V.S., Kumar, C.N. Bio-Inspired and Trust Based Clustering Routing Protocol for Hybrid MANETs.*Wireless col Commun* (2024). https://doi.org/10.1007/s11277-024-11724-w