International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 07th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-1

DOI: 10.48047/IJIEMR/V12/ISSUE 01/50

Title **Framework, Algorithms, And Validation For Sensor Attack Detection And Isolation In Autonomous Vehicles**

Volume 12, Issue 1, Pages: 546-553

Paper Authors

Mrs. K. Lavanya. V. Laxmi mounika, k. Shreya, A. Raveena

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Framework, Algorithms, And Validation For Sensor Attack Detection And Isolation In Autonomous Vehicles

Mrs. K. Lavanya. Assistant professor, Dept. of Information Technology, Sridevi Women's Engineering College, Hyd. teachinglavanyak@gmail.com

V. Laxmi mounika, B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

k. Shreya , B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

A. Raveena , B.Tech., Dept. of Information Technology, Sridevi Women's Engineering College, Hyd.

ABSTRACT— In this work, we delve into the issue of cyber security for autonomous cars, focusing specifically on how they fare when subjected to sensor assaults. In order to ensure safe localization of autonomous cars, a model-based framework is suggested that can detect sensor assaults and trace them back to their origins. Redundant sensors are used to make the vehicle more secure against cyberattacks. These sensors constantly monitor the car's position in real time. To identify outliers in every sensor reading, we build a network of attack detectors using a mixture of an extended Kalman filter (EKF) and a cumulative sum (CUSUM) discriminator. Recursively estimating the vehicle's position and orientation using EKFs allows for each CUSUM discriminator to analyse the residual generated by its combined EKF and identify any potential discrepancies between the sensor measurement and the expected pose derived from the vehicle's mathematical model. By introducing a secondary detector that combines data from many sensors, we can keep an eye on any discrepancies in the data collected by different instruments. We build a rule-based isolation method to single out the aberrant sensor based on the data from all of our detectors. On real-world vehicle data, our suggested methodology has been shown to be effective.

INTRODUCTION

There has been considerable progress in autonomous driving technology in recent years, and some driverless cars have already entered public use. Allowing for Intelligent Systems disasters of the worst kind Recent research has shown that autonomous cars might be vulnerable to sensor assaults. Examples include GPS spoofing and wireless network attacks.capable of manipulating GPS data. Point clouds may be altered by LiDAR spoofing attacks to remove or introduce fictitious impediments in the driver's path. Spoofing attacks are a method of tricking optical flow sensors . In addition, it has been shown that the widely used Robot Operating System (ROS) robotics middleware suite is susceptible to hacks in which the sensor readings may be manipulated .Therefore, it is crucial to create strategies for the protection of cars from real-time sensor assaults, which falls within the remit of cyber-security in the aforementioned literature. In response to the aforementioned difficulty, the present research investigates the means by which cyberattacks on the localization sensors used in autonomous cars (such as GPS and LiDAR) might be detected and identified.Research groups have paid a lot of attention to the cyber-security of autonomous cars during the last decade, particularly over the past five years. The purpose of is to serve as a whistleblower on cyber-security dangers to automated cars by investigating possible cyber-attacks on autonomous vehicles and identifying mitigating techniques to mitigate these vulnerabilities.To better comprehend cyber-security of autonomous cars, provides a thorough taxonomy of threats and accompanying response measures. In the author conducts a thorough literature analysis, summarising the discovered weaknesses and developing solutions to address them in autonomous cars. Many solutions have been proposed to the cyber-security issue of autonomous vehicles; these solutions can be broken down into two broad categories: information-oriented and control-oriented. Information-oriented solutions focus on achieving security goals through the use of data security techniques like encryption, user authentication, plausibility checking, etc. Normal examples of labour may be found in the references [8–13]. As data monitoring is the foundation of such methods, robust defences may be constructed against intruders and other external threats. Information-oriented defences are effective against external attackers that lack access to on-board cyber and physical components of the vehicle but have access to, and knowledge of, the cryptographic techniques used in the system.

RELATED WORK

“Capturing and controlling unmanned aircraft by GPS spoofing,"

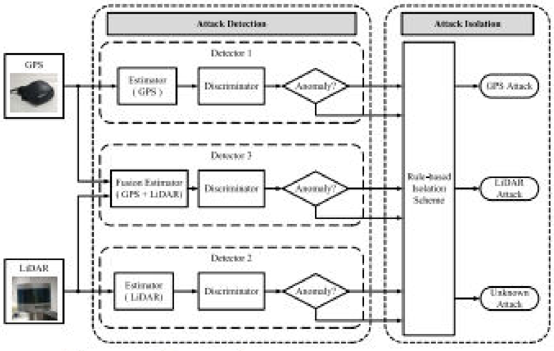
Both the theory and practise of capturing and controlling UAVs by spoofing their Global Positioning System (GPS) signals are discussed and shown. Examining how susceptible UAVs are to erroneous GPS signals is the focus of this study. This study does two things: (1) it lays out the circumstances under which a GPS spoof may be used to successfully capture an unmanned aerial vehicle, and (2) it investigates the many ways in which a spoof might then exert control over the captured UAV. When a spoofer is able to reliably predict the UAV's location and speed, they have "caught" the UAV. In post-capture control, the spoofer tampers with the UAV's genuine status, which might send it on a course significantly off its original flight plan without raising alarms. The spoofer's efforts to elude detection by the target GPS receiver and by the target navigation system's state estimator, which is assumed to have access to data from non-GPS navigation sensors, separate the overt and covert spoofing tactics under consideration. Spoofer capability for stealthy capture of a moving target is evaluated by analysing and testing tracking loops from GPS receivers. This paper analyses and simulates post-capture control situations involving a spoofer and an unmanned aerial vehicle. In a real-world scenario, a rotorcraft UAV is captured and piloted with just the most basic controls, leading to an inevitable crash due to irreparable navigational mistakes.

“Autonomous vehicles vulnerable to 'adversarial sensor attacks on LiDAR-based perception”

One of the most important components of autonomous vehicles is perception, which uses sensors like cameras and LiDARs (Light Detection and Ranging) to analyse the road ahead. Multiple previous initiatives have studied the security of perception systems because of its direct influence on traffic safety. We conduct the first security analysis of LiDAR-based perception in AV situations, which is very relevant but has not been thoroughly investigated before. We simulate assaults using LiDAR spoofing, with the purpose of simulating impediments in front of an autonomous vehicle (AV) that has been targeted. As a result of the machine learning-based object identification method, we conclude that indiscriminately using LiDAR spoofing is not adequate to accomplish this objective. Thus, we investigate the potential for tactically guiding the faked assault to deceive the AI system. This is framed as an optimization issue, and we develop models for the input perturbation function and the goal value. To boost attack success rates to roughly 75%, we also identify the constraints of optimising the issue directly and develop a method that combines optimization with global sampling. As a case study, we develop and assess two assault scenarios that may compromise road safety and mobility in order to better comprehend the effect of an attack at the level of the driving decisions made by autonomous vehicles. We also go through defensive strategies at the levels of AV systems, sensors, and ML models.

METHODOLOGY

It is possible that cyberattacks against autonomous driving apps may cause fatal accidents due to sensor abnormalities. Detecting assaults is essential for the protection of pedestrians and transit users.within a reasonable amount of time. Additionally, it is important to identify the sensors that were the cause of the anomaly in order to assist future recovery and improve the safety of the autonomous vehicle system. From these considerations, the paper's explored sensor attack detection and isolation issue may be expressed as follows.because the adversary cannot apply an assault prior to the vehicle's initialization in practical contexts.Furthermore, the expected actuator command must not be weakened in any way. In fact, anomalies may be identified regardless of whether the sensor measurement or the actuator instruction is abnormal, provided that the detector is triggered by the difference between the anticipated state and the sensor measurement. However, the detector fails if the deviation is not sufficiently obvious, such as when an attacker manipulates sensor measurement and actuator command in accordance with the mathematical model of the vehicle so that they are consistent. This very unusual case is not taken into account in this article.

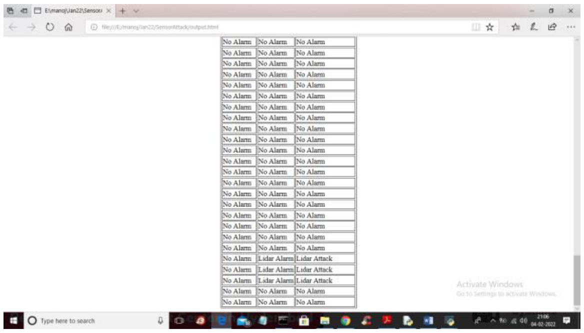


The proposed framework.

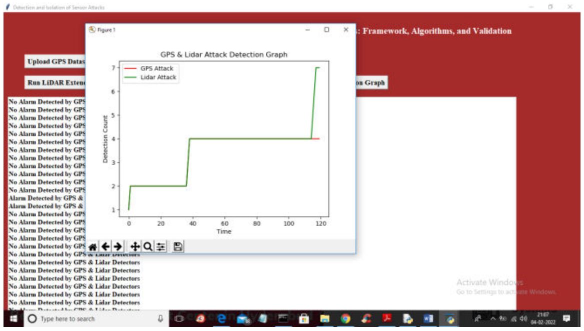
RESULT AND DISCUSSION

Select the GPS data you want to transfer, then click the Open button to load it. The GPS dataset was loaded, and then the LIDAR dataset was uploaded using the

Upload LIDAR Dataset button and a.csv file was loaded using the Open button. The 'Run GPS Extended Kalman Filter' button is used to process EKF on GPS data once a lidar dataset has been imported. source coordinates Next stop, as anticipated by EKF, is Use an Extended Kalman Filter (EKF) on the raw LIDAR data. The anticipated position of EKF is quite close to the actual position, as can be seen by comparing the two numbers. Execute RULES to trigger attack warning based on CUSUM detector's rule-based analysis of data for deviations from expected values.



No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm
No Alarm	Lidar Alarm	Lidar Attack
No Alarm	Lidar Alarm	Lidar Attack
No Alarm	Lidar Alarm	Lidar Attack
No Alarm	No Alarm	No Alarm
No Alarm	No Alarm	No Alarm



No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
Alarm Detected by GPS &
Alarm Detected by GPS &
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS
No Alarm Detected by GPS & Lidar Detectors
No Alarm Detected by GPS & Lidar Detectors
No Alarm Detected by GPS & Lidar Detectors
No Alarm Detected by GPS & Lidar Detectors
No Alarm Detected by GPS & Lidar Detectors
No Alarm Detected by GPS & Lidar Detectors
No Alarm Detected by GPS & Lidar Detectors

assault, and the green line is a Lidar strike

CONCLUSION

In order to identify and separate cyberattacks on the sensors of autonomous cars, a model-based methodology is provided in this study. Using a new offensive strategy By developing a rule-based attack isolation strategy, sensor assaults can now be not only detected, but also recognised, significantly boosting the cyber security of autonomous cars. Data from actual vehicles was used in experiments that proved our suggested framework to be effective. The trials take into careful account four kinds of typical assaults, including denial-of-service, forward-denial-of-interaction, stealthy, and replay attacks, from which seven attack scenarios are developed. Experiments demonstrate that a GPS stealthy assault, which may avoid the monitoring of the usual model-based method, can be detected by inserting an additional detector which checks the discrepancy among numerous sensor data. There are still drawbacks to the suggested strategy, as discussed in Section IV-F. More work will be done in the future to fix these issues.

REFERENCES

[1] A. 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] A. Bezemskij, G. Loukas, R. J. Anthony, and D. Gan, "Behaviourbased 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] A. Bezemskij, G. Loukas, D. Gan, and R. J. Anthony, "Detecting cyberphysical 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] A. 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] I. 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] A. 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. [Online]. Available: https://www.autoware.org/
[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.