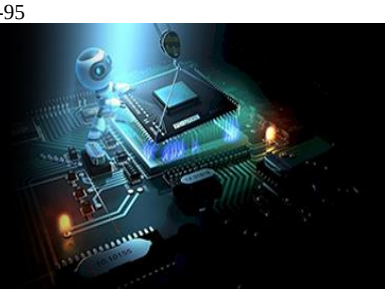
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
www.computersciencejournals.com/ijecs
IJECS 2024; 6(2): 91-95
Received: 01-05-2024
Accepted: 10-06-2024

G Karunakar
Assistant Professor, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad, Telangana, India

Huzaifa Tarannum
Student, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad, Telangana, India

K Nandana Sri
Student, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad, Telangana, India

G Shravani
Student, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad, Telangana, India

Corresponding Author:
G Karunakar
Assistant Professor, Department of CSE, Malla Reddy Engineering College for Women, Autonomous, Hyderabad, Telangana, India

Applying the Kalman filter algorithm on autonomous vehicles: Framework and validation for sensor attack detection and isolation

G Karunakar, Huzaifa Tarannum, K Nandana Sri and G Shravani

DOI: https://doi.org/10.33545/26633582.2024.v6.i2b.128

Abstract
Under sensor assaults, this study explores the cyber-security dilemma of autonomous cars. Secure localization of autonomous cars is a top priority, thus we provide a model-based system that can detect sensor assaults and pinpoint their origins. Introducing sensor redundancy, or the deployment of numerous sensors, each of which offers real-time posture observations of the vehicle, ensures that the vehicle is resistant against cyber-attacks. A set of attack detectors, which includes an extra Kalman filter (EKF) and the cumulative sum (CUSUM) discriminator, is created to identify outliers in every sensor reading. Using EKFs, we can recursively estimate the vehicle's position and orientation. Then, to find any discrepancy between the sensor reading and the predicted pose based on the vehicle's mathematical model, we can use each CUSUM discriminator to analyse the residual produced by its combined EKF. The introduction of an auxiliary detector that combines data from many sensors allows for the monitoring of inconsistencies in the results obtained from these sensors. An isolation strategy based on rules is created to find the source of the aberrant sensor using the data from all the detectors. Using actual car data, we proved that our suggested architecture works.

Keywords: Autonomous vehicles, Kalman filter, sensor attack detection, sensor redundancy

Introduction
There has been tremendous progress in self-driving technology in recent years, and some driverless cars are already on public roads. Autonomous vehicle systems use a multitude of sensors—GPS, LiDAR, cameras, etc.—to determine their position and understand their surroundings, paving the way for intelligent transportation. This makes potential weak spots more accessible to cybercriminals. Automobiles, once compromised, could exhibit strange conduct that leads to inconvenient outcomes or even deadly collisions. A small number of investigations have shown that autonomous cars might be vulnerable to sensor assaults. One method that may be used to manipulate GPS data is GPS spoofing. By inserting or removing real or false impediments from the vehicle's path, LiDAR spoofing attacks may alter point clouds. Potentially susceptible to spoofing attempts are optical flow sensors. The Robot Operating Systems (ROS), a popular robotics middleware suite, has been shown to be susceptible to hacks that might alter sensor data. Thus, it is crucial to create strategies for safeguarding automobiles from real-time sensor assaults, a subfield of cyber-security in relevant literature. Based on the problem statement, this article investigates how to identify and prevent cyberattacks on the location sensors used by autonomous cars, namely GPS and LiDAR. Research groups have paid a great deal of attention to the topic of bear-security in autonomous cars throughout the last decade, particularly in the last five years. Identifies possible cyber-attacks on autonomous cars and researches mitigating techniques to counter them; blows the whistle on these dangers to automated vehicle cyber security. As a means of better comprehending the cyber-security of autonomous cars, provides a thorough taxonomy of assaults and associated defensive strategies. This provides a comprehensive literature study on autonomous cars, summarizing the vulnerabilities found in the literature and offering solutions to protect them. A number of methods have been suggested to deal with the cyber-security issue with autonomous cars; these methods may be broadly grouped into two groups: those that focus on information and those that focus on control. Encryption, authentication of users, plausibility testing, and other data security methods are used by

information-oriented approaches to accomplish security goals. Given that data monitoring is at the heart of these techniques, robust defences may be put in place to ward off outsiders. The defences set up by information-oriented techniques would be breached, nevertheless, by internal attackers who are familiar with the system's cryptographic processes and have access to the vehicle's cyber and physical components. Also, these methods don't take into account how the car interacts with the real environment. Complementary to this, control-oriented methods have been suggested for investigating the physical dynamics of the control system and how cyber-attacks influence them. In order to make the self-driving vehicle system more resistant to harmful cyber-attacks, control-oriented approaches build security tools by analysing the effects of attacks using vehicle and attack system models. This adds another layer of defense to the already robust information-oriented approaches. There are two primary categories of control-oriented approaches: data-driven and model-based. Data-driven methods match real-time web data with historical records of assaults in order to solve the attack detection issue using machine learning. When it comes to real-time localization systems, for instance, eight algorithms for supervised learning have been examined and tested for the purpose of detecting DoS and spoofing attacks using actual data acquired by a wheeled robot. To guarantee the cyber-security of autonomous cars, a technique that utilizes convolutional neural network technology (CNN) is created to analyze time-series data collected from various speed sensors in order to spot and identify anomalies. The best way for autonomous cars to fuse sensors in the event that any of them are compromised is learned using deep reinforcement learning algorithms, as mentioned in the reference. These methods work well with assaults that are already present in the training data, but they won't be able to detect new types of attacks. The generalizability of data-driven methods is further compromised by the random nature of cyber-attacks, which makes training data production an extremely difficult operation. Other research, in an effort to streamline the process, uses one-class categorization rather than assault type identification. To be more specific, computers are trained using normal data alone, and only then are anomalies detected. The authors suggest an internet-based anomaly detection framework that uses learning to keep an eye on the mappings between sensor data, actuator commands, and future sensor data in order to spot any problems with the system as a whole. Using a One Classes Support Vector Model (OCSVM) model, linked autonomous cars may identify unusual sensor readings in. It is straightforward to adopt these simplified data-driven strategies since they simply need typical data for model training. Be that as it may, these techniques are limited to detecting anomalies and not determining their origin. The algorithms' inherent unpredictability is further amplified by the fact that characteristics employed in model training are not easy to extract.

Related work

"Grappling and controlling unmanned aircraft through GPS spoofing"

We examine and show how to implement the idea and practice of capturing and controlling UAVs via GPS signal spoofing. Investigating the susceptibility of UAVs to false GPS signals is the primary objective of this study. The purpose of this study is twofold: first, to lay out the groundwork for capturing UAVs using GPS spoofing; and second, to investigate the spectrum of post-capture control options available via spoofing. Once a faked UAV can finally provide accurate predictions of the UAV's location and velocity, it is termed captured. The spoofing compromises the UAV's real status during post-capture control, which might cause it to deviate significantly from its flight plan with triggering any alarms. There are two types of spoofing tactics that are taken into account: overt and covert. The former tries to avoid detection by the target's GPS receiver, while the latter uses the target navigational system's position estimator, which is assumed to have access to data from non-GPS navigation sensors. The effectiveness of the spoofing to secretly capture a moving object is evaluated by analysing and testing GPS receiver tracking loops. In order to investigate realistic post-capture control situations, we analyse and simulate the combined flight characteristics of a UAV and spoofing. A rotorcraft UAV crashes during a field test showing just basic control and capture capabilities. The pilot made irreparable navigational mistakes.

"Environmental threat to LiDAR-based autonomous driving perception systems"

An essential component of AVs is perception, which uses sensors like as camera and LIDARs (Light Detecting and Ranging) to comprehend the road ahead. The security of vision systems has been the subject of several previous attempts to examine because of the direct influence it has on road safety. Here, we conduct the first security analysis of perception generated by LiDAR in AV contexts, a crucial but so far untouched area of research, in contrast to previous work that has focused on camera-based perception. We model the threat as LiDAR spoofing attacks and aim to spoof obstacles at the front of the target AV. Because of a machine learning-based object recognition process, we discover that just using LiDAR spoofing is not enough to do this. As a result, we investigate if it is possible to deliberately manipulate the simulated assault in order to deceive the machine learning algorithm. To represent the input disruption function and the goal function, we create an optimization problem formulation and apply it to the job. We further determine that optimizing the issue directly has its limits and instead devise a method that merges optimization with global sampling; this increases the assault's rate of success to around 75%. We build and assess two assault scenarios that might harm road safety or mobility as an example to learn about the effects of attacks at the level of autonomous vehicle driving decisions. Our discussion also covers defense-related topics at the levels of AV systems, sensors, and machine learning models.

"Attacks on unmanned aerial vehicle control using sensor input spoofing"

Interest in driverless cars and robotics has recently skyrocketed. There is an astounding diversity of planned deployments for autonomous vehicles, ranging from the Google self-driving automobile to autonomous delivery robots to hobbyist UAVs. It is critical to guarantee that these vehicles can securely plan and carry out itineraries. Our paper's main takeaway is that autonomous cars' navigation sensors are a potential entry point for hostile control. The adversary may establish a subconscious controlling loop on

the victim by manipulating the victim's surroundings, thanks to their firsthand understanding of how detector algorithms function. Our assault, which we term a sensor feedback spoofing attack, is built on this concept. We show that the widely used Lucas-Kaneda technique for optical flow detection may be attacked by faking sensor inputs and describe how an attacker can simulate optical flow manipulation. Additionally, we show that our visual input from sensors spoofing attack successfully counters two consumer-grade UAVs, namely the AR. Drone 2.0 with the APM 2.5 Adopter. Lastly, we provide a strategy to protect optical-flow sensors against this kind of assault, which use the RANSAC algorithms and an improved weighted RANSAC algorithms to combine sensor readings.

"A perspective on security in robotics research: scanning the internet for ROS"

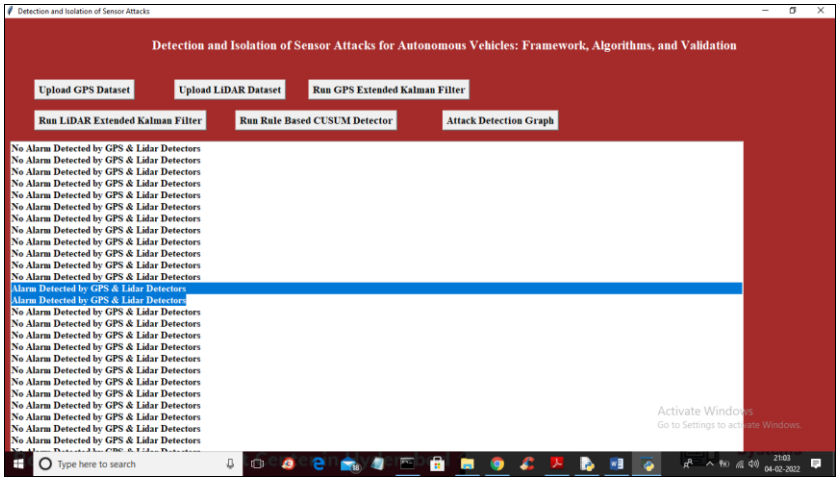
Due to their ability to interact with the actual environment, robots pose unique security challenges. We detail the outcomes of an Internet-wide search for instances of ROS, a popular robotics software platform, and using IPv4 addresses. Our research has shown that there are many ROS-supporting servers available via the open Internet, which means that anyone may have access to mechanical sensors and actuators. We were capable of to read data from image sensors and control a real robot at a university lab in the US and a proof of topic, all with the approval of the appropriate experts. This document provides a synopsis of our results, including topics such as the technique we used, the locations for publicly-accessible platforms, the data types of sensors and actuators, and the various robots and sensors that our scan found. For future prevention of such security vulnerabilities, we also provide guidance on recommended practices.

Methodology

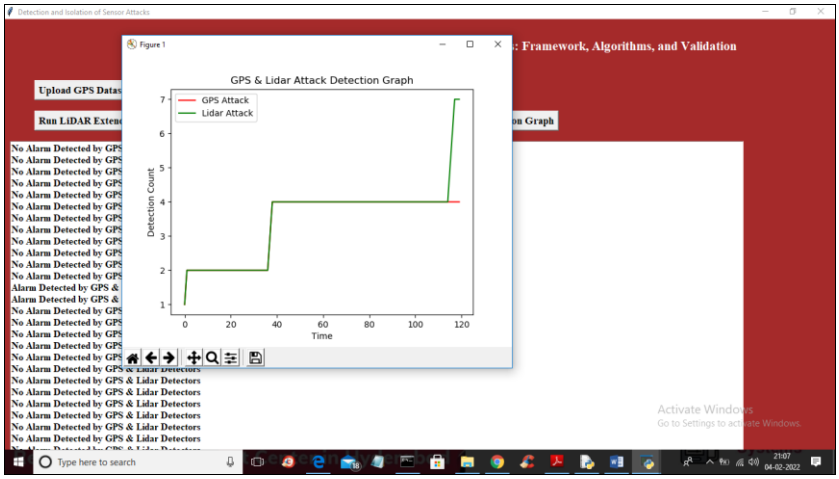
1) GPS Dataset Upload: This module will be used to upload the Google Maps dataset to the application.
2) The LiDAR dataset will be uploaded to the application using this module.
3) Implement the GPS Expanded Kalman Filter: this component will implement the Kalman filter method to forecast the whereabouts of vehicles by tracking their initial GPS coordinates.
4) Execute LIDAR Extend Kalman Filter: this component will implement the Kalman filter method to forecast where vehicles are by keeping tabs on their initial LIDAR positions.
5) The Run Rule on CUSUM Detector module applies CUSUM to the EKF data in order to identify variations; an attack warning will be sounded in the event that very large variations are identified.
6) Graph for Attack Detection: Total assaults identified by LIDAR as well as GPS will be shown using this module.

Results and Discussion

You may submit your GPS dataset by clicking the "Upload GPS Dataset" button in the results.



It is clear from the blue language on the above screen that CUSUM has implemented criteria to identify attacks based on each latitude and longitude; nevertheless, in other records, there is no alarm identified.



From 0 to 120 records, GPS (detector 1) recorded a total of 4 assaults, while lidar (detector 2) identified a total of 7 attacks. The x-axis indicates time, and the y-axis shows the count of attacks. The line in red represents GPS attacks, while the line in green represents lidar attacks.

Conclusion

To identify and separate cyber-attacks on autonomous vehicle sensors, this study proposes a model-based architecture. The cyber-security of self-driving vehicles is significantly improved by using a rule-based assault isolation strategy that uses an institution of attack detector to detect and identify sensor assaults. Our suggested approach has been shown effective via experiments run on actual car data. Seven different assault scenarios were developed based on the thorough consideration of four prevalent kinds of attacks in the experiments: denial-of-service (DoS), foreign direct interference (FDI), stealthy, and replay attacks. The results demonstrate that a GPS stealthy assault may be identified, which can avoid detection by the traditional model-based method, by including an additional detector that tracks the discrepancy between the readings from various sensors. The suggested technique is not without its flaws, as mentioned in Section IV-F. These downsides will be worked on in the future.

References

1. Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE. Unmanned aircraft capture and control via GPS spoofing. J Field Robot. 2014;31(4):617-636.
2. Cao Y, Liu Y, Zhang J, Yang Y, Zhang L. Adversarial sensor attack on LiDAR-based perception in autonomous driving. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security; London, UK; c2019. p. 2267-2281.
3. Davidson D, Wu H, Jelinek R, Singh V, Rosengard T. Controlling UAVs with sensor input spoofing attacks. In: Proceedings of the 10th USENIX Workshop on Offensive Technology (WOOT); Austin, TX; c2016. p. 221-231.
4. DeMartini N, Telex S, Kemiris VP, Kendari G, Fonseca R. Scanning the Internet for ROS: A view of security in robotics research. In: Proceedings of the International Conference on Robotics and Automation (ICRA); Montreal, Canada; c2019. p. 8514-8521.
5. Petit J, Shadier SE. Potential cyberattacks on automated vehicles. IEEE Trans Intell Transp Syst. 2015;16(2):546-556.
6. Thing VLL, Wu J. Autonomous vehicle security: A taxonomy of attacks and defences. In: Proceedings of the IEEE International Conference on Internet of Things (iThings); Chengdu, China; c2016 Dec. p. 164-170.
7. Parkinson S, Ward P, Wilson K, Miller J. Cyber threats facing autonomous and connected vehicles: Future challenges. IEEE Trans Intell Transp Syst. 2017;18(11):2898-2915.
8. Brzeski A, Loukas G, Anthony RJ, Gan D. Behaviour based anomaly detection of cyber-physical attacks on a robotic vehicle. In: Proceedings of the 15th International Conference on Ubiquitous Computing and Ambient Intelligence: Cybersecurity; 2016 Dec; Tenerife, Spain. p. 61-8.
9. Brzeski A, Loukas G, Gan D, Anthony RJ. Detecting hyperphysical threats in an autonomous robotic vehicle using Bayesian networks. In: Proceedings of the IEEE International Conference on Internet of Things (iThings); London, UK; c2017 Jun. p. 98-103.
10. Olivetol M, Octagon O, Rigato L, Blois D, Facinelli A, Fiocchi L. A comparative analysis on the use of autoencoders for robot security anomaly detection. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS); Macau, China; c2019 Nov. p. 984-989.
11. Suo D, Samra SE. Real-time trust-building schemes for mitigating malicious behaviours in connected and automated vehicles. In: Proceedings of the IEEE Intelligent Transportation Systems Conference (ITSC); Auckland, New Zealand; c2019 Oct. p. 1142-1149.
12. Jiang F, Qi B, Wu T, Zhu K, Zhang L. CPSS: CP-ABE based platoon secure sensing scheme against cyber-attacks. In: Proceedings of the IEEE Intelligent Transportation Systems Conference (ITSC); Auckland, New Zealand; 2019 Oct. p. 3218-3223.
13. Changeable R, Malik H. LiDAR data integrity verification for autonomous vehicle. IEEE Access. 2019;7:138018-138031.
14. Kwon C, Liu W, Hwang I. Security analysis for cyber-physical systems against stealthy deception attacks. In:

Proceedings of the American Control Conference; Washington, DC; c2013 Jun. p. 3344-3349.
15. Sánchez HS, Rotunda D, Escobedo T, Puig V, Quevedo J. Bibliographical review on cyber-attacks from a control oriented perspective. Annu Rev Control. 2019;48:103-128.
16. Guerrero-Higuera ÁM, DeCastro-García N, Magellan V. Detection of cyber-attacks to indoor real time localization systems for autonomous robots. Robot Auton Syst. 2018;99:75-83.
17. van Week F, Wang Y, Khujand A, Masoud N. Real-time sensor anomaly detection and identification in automated vehicles. IEEE Trans Intell Transp Syst. 2020;21(3):1264-7126.
18. Ferdowsi A, Chillida U, Saad W, Mandaya NB. Robust deep reinforcement learning for security and safety in autonomous vehicle systems. In: Proceedings of the 21st International Conference on Intelligent Transportation Systems (ITSC); Maui, HI; c2018 Nov. p. 307-312.
19. Rasheed I, Hu F, Zhang L. Deep reinforcement learning approach for autonomous vehicle systems for maintaining security and safety using LSTM-GAN. Veh Commun. 2020;26:100266.
20. Patel N, Sirisena AN, Chromans A, Krishnamurthy P, Khor rami F. Adversarial learning-based on-line anomaly monitoring for assured autonomy. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS); Madrid, Spain; c2018 Oct. p. 6149-6154.
21. Wang Y, Masoud N, Khujand A. Real-time sensor anomaly detection and recovery in connected automated vehicle sensors. IEEE Trans Intell Transp Syst. 2021;22(3):1411-1421.
22. Abdullahi Biron Z, Dey S, Pisa P. Real-time detection and estimation of denial of service attack in connected vehicle systems. IEEE Trans Intell Transp Syst. 2018;19(12):3893-902.
23. Mosaiced E, Yang F, Han Q-L, Ge X, Lactic L. Distributed cyber-attacks detection and recovery mechanism for vehicle platooning. IEEE Trans Intell Transp Syst. 2020;21(9):3821-3834.
24. Sabella skate G, Ng GS, Ruth's J, Mathur A. A comprehensive approach, and a case study, for conducting attack detection experiments in cyber-physical systems. Robot Auton Syst. 2017;98:174-191.
25. Keiper A, Mousasi M, Scherer S. Automatic real-time anomaly detection for autonomous aerial vehicles. In: Proceedings of the International Conference on Robotics and Automation (ICRA); Montreal, Canada; c2019 May. p. 5679-5685.