ATTACKS ON SENSORS FOR AUTONOMOUS VEHICLES: DETECTION AND ISOLATION

DR. P. Sunil Kumar, M. Divya Bhanu , G. Vijitha ,

1 Assistant professor, Department of Electronics and Communication Engineering, Sri devi Women's Engineering College, Hyderabad, India.

2,3,4 B. tech Students Department of Electronics and Communication Engineering, Sri devi Women's Engineering College, Hyderabad, India.

1,2,3,4 Department of Electronics and Communication Engineering, Sri devi Women's Engineering College, Hyderabad, India.\

1 psunilkumar.ece@gmail.com

2 reddydivyabhanu@gmail.com

3 vijithagollagudem17@gmail.com

Abstract: This research looks on the cyber security threat posed by sensor assaults to autonomous cars. Specifically, a model-based strategy is proposed to allow safe localization of autonomous vehicles by identifying the origins of sensor assaults. As a countermeasure against cyberattacks, we propose sensor redundant work, or the use of many sensors to monitor the vehicle's position in real time. Banks of attack detectors are constructed using a Kalman filter with an extension (EKF) and an overall sum (CUSUM) distinction to identify outliers in sensor readings. The recursive EKFs are used CUSUM discriminators are built to analyse the remaining energy produced by their combined EKF in order to spot any deviation of the sensor's output from the projected ask derived from a numerical model of the vehicle, allowing for more accurate position and orientation estimates. To keep an eye on the discrepancy between various sensors' readings, a new type of detector is devised that combines information from many sensors. On the basis of these rules, an isolation strategy is developed to identify the offending sensor. results from each and every detector. Our proposed framework has been shown to be useful based on data from actual automobiles.

Key words: Cyberattack, anomaly detection, autonomous vehicle, and sensor assault.

Introduction: Some driverless cars are already out and about on the roads thanks to the rapid development of autonomous driving technology in recent years. To enable cognizant movement, autonomous vehicle systems rely on a variety sensors consisting mostly of GPS, LIDAR, cameras, and other similar devices.

Thiswidens the scope of potential vulnerabilities that might be exploited by malicious assaults. Attacks on vehicles might cause them to act in unexpected ways, which could have far-reaching consequences. catastrophic mishaps are also possible. Some research to this point has demonstrated that sensor assaults against autonomous cars are possible; for instance, GPS spoofing can render GPS readings invalid [1]. Points clouds generated by LiDAR spoofing attacks may be used to mask the location of real barriers, and replacement ones can be placed in their stead. [2]. Optical flow sensors are vulnerable to spoofing attempts [3The recent discovery that the widely used robot operating system (ROS) is susceptible to cyber-attacks that may modify sensors in real-time highlights the critical need of ensuring the system's cyber-security. This research was inspired by the aforementioned issue, with the goal of detecting and identifying cyber-attacks aimed at the positioning sensors used by autonomous automobiles. These sensors include the global positioning system (GPS) and the lidar (LiDAR). Over the last decade, and especially in the past few months, academics have paid a lot of focus to the safety elements of autonomous automobiles.Cyber security watchdog [5] looks at the prospect of cyber attacks on driverless cars and suggests countermeasures to keep them safe. Cybersecurity threats to autonomous cars are categorised and defences against them are discussed in detail in [6]. In [7], a comprehensive literature review is provided, outlining the observed vulnerabilities and developing mitigating solutions for autonomous vehicles. Information-oriented gets closer use data security techniques like the use of encryption, authorization of users, plausibility testing, etc., to achieve security goals; These are only a few of the numerous solutions offered to ensure the security of autonomous vehicles while they are connected to the internet. The emphasis of control methods is on the vehicle's actual safety. Examples of typical work can possibly be observed in [8]–[13]. The primary idea behind these techniques is surveillance of data, which provides strong defences against intruders and other outside threats. However, the defences set up by information-oriented techniques would be easily circumvented by internal attackers who are aware of the cryptography method and have authority to interact with on-board cyber and physical parts of the vehicle. More importantly, the procedures in question do not account for the vehicle's real interactions with the environment. with the environment. Complementing these methods are command-oriented ones, which focus on learning from cyberattacks to improve control system physical dynamics [14]. Using models of both the attacked system and the vehicle, control-oriented methodologies develop protective measures. These methods supplement information-based defences and fortify the autonomous vehicle's system against harmful intrusions. Data-driven and model-based techniques are the two most common types of control-oriented methods used today. By using learning systems to compare real-time data with records relating to specific assaults, data-driven methods address the problem of attack detection. In [16], for example, eight supervised algorithms for learning are evaluated based on real-world data gathered through a wheeled robot to spot Denial of service(DOS) & spoofing incidents on RTLS. A multilayer neural network (CNN)-based method for anomalies detection and recognition was developed in [17] by analysing time-series data from a large number of speed sensors to ensure the cyber-security of autonomous cars. In the case that any of an autonomous vehicle's sensors are compromised, researchers recommend using deep reinforcement learning techniques, as seen in references [18], [19]. However, these techniques can't spot new assaults since they only work with ones that are identical to the training data. Additionally, given the potential randomness of cyberattacks, the creation By continuously monitoring the connection between sensory data and actuators command and between actuator order and future sensor data, anomalies in the entire system may be detected using a learning-based online detection of anomalies technique, as proposed in [20]. To identify sensor abnormalities, a One class aid vector Machine (OCSVM) model is integrated into a network of linked autonomous vehicles in [21]. These condensed data-driven solutions are easy to implement since regular data can be used to train the models. However, these methods can only detect the aberration; they cannot locate its source. The complexity of feature extraction for model training also increases the unpredictability of these methods.

Instead, model-based techniques, the usefulness of which has been verified in long-term practises, detect when sensor data deviates from the predicted behaviour determined from the theoretical representation of the vehicle. In [22], the authors propose a real-time method for detecting distributed denial of service (DDoS) assaults in modern automobiles. This method can detect when a denial of service (DoS) assault is launched against a vehicle's linked system and calculate roughly how much damage will be inflicted. To identify assaults that damage the communication infrastructure and on-board sensors of a vehicle platooning system, [23] develops a novel distributed attack detection approach. However, the proposed algorithms in [22, 23] are mathematically sound and provide adequate performance, they are not supported by substantial data from real vehicle testing. Although not directly related to the problem at hand, they also plan to address attack detection concerns related to vehicle platooning. Reference The CNN-based detector is followed by a typical model-based technique, as shown in [17], which employs a Kalman filter and a 2-detector.In the face of an imminent wall, seven methods of anomaly detection are available for use by differential-drive mobile robot sensors. As stated and implemented in [24], contexts. Since it only takes into account basic applications, it is challenging to expand it to different circumstances. In [25], a real-time method for spotting mundane tasks on board an airliner is presented. As a means of characterising the connection, the suggested method uses an infinitely repeating least squares algorithm. between correlated input-output pairs, which is then used to spot outliers. True negatives for nonlinear systems are possible with this method because of the underlying assumption that both inputs and outcomes are linear. All of the aforementioned model-based techniques [17], [24], and [25] follow the same basic format, which involves a comparison between the measured value and the state predicted by the model of the system when uncertainty outweighs the effect of an assault. Traditional model-based detectors may miss the impact of assaults due to discrepancies between the measured and predicted states. More This issue has to be fixed so that autonomous vehicles may function online safely. The online safety for autonomous vehicles has recently been studied from a game-theoretic perspective [18], [19]. Plans based on games theory have historically struggled due to the necessity of taking into consideration the equilibrium's presence. Despite the lack of equilibrium, this study presents a model-based method for detecting and distinguishing cyberattacks made against the sensor networks of autonomous cars. The suggested architecture incorporates a number of sensors, all of which can provide continuous measurements of the vehicle's attitude. To analyse the trustworthiness of data from multiple sensors, we provide an appraiser based on the grew Kalman filter (EKF); its structure is similar to that of each detector, but it combines observations from various sensors to monitor any deviance from the believed pose calculated from the theoretical model of the vehicle. A rule-based isolation approach is created to identify the malfunctioning sensors through the detection outputs. The proposed method was meant to be tested with an actual database from a self-driving automobile.

The primary results of this study are outlined below.

It is recommended that autonomous cars use a multi-detector configuration to detect sensor assaults. The key difference between this design and previous model-based methods is the incorporation of a new supplementary detector that monitors discrepancies in data from several sensors. relying on the output from several detectors, a rule-based segregation technique is established which may rapidly identify the reason for aberrant sensors, making detection of stealthy assaults simpler than with conventional approaches. The majority of the prior research in this area employs simulated datasets, however the suggested technique is confirmed using real vehicle data, as indicated in an up-to-date study [26].

Everything else here is simple and well-organized. In the second section, we provide a mathematical description of the issue. We provide the suggested framework in Section III, the experimental findings in Section IV, and our conclusions and suggestions for the future in Section V.

Literature survey: The concept and technique of capturing and controlling UAVs is shown by an examination and demonstration of GPS signal spoofing, Similarly to what A.J. Kerns[1], D.P. Shepard Events, J.A. Bhatti, and T.E. to Humphreys have recommended. This research aims to learn how susceptible UAVs (unmanned aerial vehicles) are to inaccurate GPS readings.

A hostile sensor attack against LIDAR-based perception was proposed by Y. Cao et al. for the field of autonomous driving.[2] The ability to see their environment through sensors like cameras and LIDARs (light detection and ranging) is crucial to Avs. The safety of mental systems has been studied before because of its direct effect on transportation security. Although much research has been done on camera-based seeing, we provide the first comprehensive security analysis with LIDAR-based recognised in AV contexts.

To gain command of UAVs, an attack method based on forging sensor inputs has been proposed by Davidson as he H. Wu, R. Jelinek, M. Singh[3], and T.Ristenpart.This modern era has been a rise in fascination in autonomous robots and automobiles. Autonomous vehicles have a wide variety of possible uses, from the Android self-driving car to self-driving couriers to hobbyist unmanned aerial drones. Our paper's central argument is that autonomous cars are vulnerable to hostile control because of the navigational sensors they rely on.

Security in robots is an area that has been studied by academics including N. Delaware Marinis, S.Telex, V.P.Kemiris, G.Kendari, or R.Fonseca[4].Because robots can see as feel their surroundings, safety is a major concern in the field of robotics.As a service to the robotics community, we present the outcomes of a web-wide hunt for ROS (Robot Operative System) installations.

Two researchers, O. J. Petit and S. E. Shladover[5], have suggested possible attacks on autonomous vehicles. Auto automation has been a primary use of ITS technology since its inception in the mid-1980s. For the most part over this time period, it has been seen as a theoretical concept with a long way to go before it is ready for implementation.

The work of J.Wu and V.L.L.[6] Consider doing an attack and defensive study on autonomous cars, in which smart mobility's emphasis on solving the issues of urban ground transport is a key factor.In this research, we categorise the many methods used to attack and defend autonomous vehicles and provide a comprehensive taxonomy for doing so.

Researchers like S.Parkinson, P.Ward, K.Wilson, etc J.Miller have all expressed concern about the cyber threats that autonomous vehicles face. and networked cars.[7] Tensions to come: More and more autonomous and connected automobiles are being developed and sold nowadays.All networked computing equipment is susceptible to cyber security threats as their connectivity grows.Furthermore, increased automation makes any threat worse by providing the attacker more opportunities to succeed in their attack.

Bezemskji, R. Loukas, R.J. Anthony, and D. Gan provided a model for the behavior-based identification of anomalies for cyber-physical attacks on a robotic vehicle[8].Any cyber attack on a cyber-physical system might have real-world repercussions, which presents a new set of security issues. Autonomous vehicles, by their very nature, represent a serious bodily hazard in the event of a disruption in their ability to communicate or process data.

In order to identify cyber-physical dangers in an R.j.Anthony, G.Loukas, D.Gan, et A.Bezemskji[9] propose using Bayesian networks in an autonomous robotic vehicle.Robotic cars, especially autonomous ones, might be appealing targets for cyberattacks or sensory channel hacks that disrupt navigation or the performance of tasks.

A number of researchers, including D.Bloisi,A.Farinelli,L.Iocchi,M.Olivato,O.Cotugno,L.Brigato,[10] have offered a comparison of autoencoder applications in robot security anomaly detection. While the public's usage of robots continues to rise, so too does the effect of cyber-security breaches.

With their CP-ABE-based platoon safe sensing system, F.Jiang, B.Qi, T.Wu, K.Zhu, and L.Zhang aim to protect networks from malicious cyber activity. Moving in a "platoon," once multiple vehicles coordinate their sensor use, improves speed and safety. If the collaborative cars don't have security insurance, a cyberattack might have catastrophic results. In this, we introduce the potentially lethal platoon manoeuvre attack.

Cyber-physical systems have been the focus of research of . Hwang, who have presented their findings on how to protect them from covert deception assaults. The problem of information security for computerized important and nuanced. The unpredictable nature of cyberattacks makes them challenging to characterize in any kind of methodical way.

Cyber-attack detection on autonomous robot real-time indoor locator systems has been proposed by The safety of online robotic systems is a major concern. Real-time locating systems are crucial for many mobile robots' ability to perform safely in a variety of environments.

A device for automated cars to detect and diagnose sensor abnormalities in real time is proposed by N. F. Van Wyke, Y. Wang, A. Khojandi, and N. Masoud. Driverless cars are predicted to revolutionize the transportation industry. industry by facilitating seamless and real-time data exchange between cars and roadside infrastructure.

Mandaya, has the potential to increase the safety and security of autonomous vehicles. Due to their reliance on sensors and network communications, self-driving automobiles (AVs) are vulnerable to cyber-physical (CP) attacks from adversaries who wish to seize control of them by altering their data.

An online anomaly monitoring system with assured independence is proposed by using adversarial learning. In order to guarantee the security and integrity of learning-based management systems throughout real time, the study suggests an environment for online monitoring. Particularly helpful for a self-driving ground vehicle. We verify the mapping in both directions: from sensor data to actuator instruction (SFAM) along with from actuators instructions to the sensor inputs (CFAM).

Observer-based strategies are introduced in this paper by to increase CAV safety and security. The AEKF may utilize this data to create a condition report that takes into account the location, speed, and volume of traffic around the vehicle.

Due to the susceptibility of vehicle platooning to cyberattacks, E. suggested a decentralized approach to detecting and recovering from such attacks. The focus of this research is on the distributed identification and recovery from assaults in a control system for a fleet of vehicles working together.

Three researchers—G. K. Rajbahadur, A. J. Maiton, and A. E. Hassan—have recommended a review of detecting anomalies in connected automotive cyber security and safety. Using anomaly detection techniques, the difficult task of protecting connected automobiles online has been taken on.We provide a classification system for the works that have come under us on this subject.9

Related work : The success of self-driving cars hinges on their ability to accurately perceive their surroundings, which is a challenging task. The perception section of an auto is built using a variety of sensors, such as LIDAR, RADAR, and others. V2x communications, OTA updates, security, remote vehicle health tracking, and so on are all managed through a variety of interfaces in autonomous cars. Wi-Fi, Bluetooth, cellular networks, and the on-board diagnosis (OBD-II) port are all examples. New attack vectors, both internal and external, are being made available by these APIs. Attackers have demonstrated their ability to exploit a variety of attack surfaces by creating attack vectors that may be used to launch both internal and external attacks.

Both internal and external parties might potentially compromise the sensor and its data. The development of countermeasures to these kinds of attacks is a vital part of making safe, trustworthy autonomous cars. If, for example, sensor data hacking is not recognised and localised, it might lead to incorrect impressions of the environment and subpar decision-making in terms of both route preparation and management. In this research, we propose a new method of semi-fragile data concealment for authenticating, detect tampering with, and localizing sensor information in real time.The sophisticated driver is utilized as a decision-making unit to test the suggested hiding data -based approach. The sensing-layer LIDAR knowledge is binary-watermarked using a method of data obfuscation based on the transmission of three-dimensional quantization indices (QIM). Analyzing the performance of an object identification system after noise reduction has been applied. The studies demonstrate that the suggested technique can identify and localize data manipulation attacks such as false object insertion (FOI) and promptly target object deletion (TOD). The ability to withstand attacks with more loudness is also evaluated. in particular, the planning and control of global positioning systems. In this research, we propose a new method of semi-fragile data concealment for authenticating, diagnosing tampering with, and localizing sensor data in real time.The sophisticated driver is utilized as a decision-making unit to test the suggested hiding data -based approach. The sensing-layer LIDAR knowledge is binary-watermarked using a method of data obfuscation based on the transmission of three-dimensional quantization indices (QIM). Analyzing the performance of an object identification system after noise reduction has been applied. The studies demonstrate that the suggested technique can identify and localize data manipulation attacks such as false object insertion (FOI) and promptly target object deletion (TOD). The ability to withstand attacks with more loudness is also evaluated. Positioning on the planet, specifically system (GPS) and light detection and ranging (LIDAR) systems, which are widely used in autonomous cars. Cyber security risks to the autonomic nervous system.

Disadvantages: less Accuracy

Less Security

Expanded facilities. More autonomous cars upon the road will likely increase the demand for infrastructure upgrades, especially for larger trucks.

In this section, we evaluate GPS and LIDAR data in real-time using one of three attack detection devices, Detectors 1 and 2 use an EKF-based estimator to pinpoint the vehicle's location and heading based on discrete GPS and LIDAR reports, while detector 3 keeps an eye on the deviation between the actual state of the vehicle and the one predicted by a mathematical model. Detector 3's EKF-based estimator combines GPS and LIDAR readings, and the detector's CUSUM discriminator determines whether or not the two sets of readings are consistent, so that any disparity between them may be tracked. Since the underlying detectors' architecture are the same across all three detectors, this section will cover the detectors' premise regardless of the detector's index.

ADVANTAGES: High security; High Accuracy;

method of lidar sensing involves pulsing thousands of heat laser beams into the surroundings and then waiting for the rays to bounce off adjacent objects.Using this module, we will visualise all assaults picked up by LIDAR and GPS on a single graph.

The following modules were developed specifically for this project: This section will be used to add GPS data to the programme. We'll use this section to import LIDAR data into the programme and upload the resulting dataset. In this section, we'll put the Kalman filter approach to work to predict car positions based on observations of real vehicle locations derived by GPS data. Conduct a LIDAR modified Kalman filter run. In this section, we'll learn how to utilise the Kalman filter method to predict where cars will be by following their tracks in LIDAR data. This section will apply the total on the two EKF data in try to find discrepancies based on a predefined set of rules. The alert will go off if any major discrepancies are discovered. Using this component, we can plot a graph of all LIDAR and GPS-detected assaults.

These are these papers main contributions, in order

It is recommended that autonomous cars have a multi-detector design to detect sensor assaults. The addition of a novel auxiliary detector assists in recognising the presence of sneaky assaults, which is regarded to be hard for conventional methods to detect, making this design a significant improvement over previous model-based approaches. A rule-based isolation strategy is developed using the data from several detectors to rapidly pinpoint the origins of faulty readings.

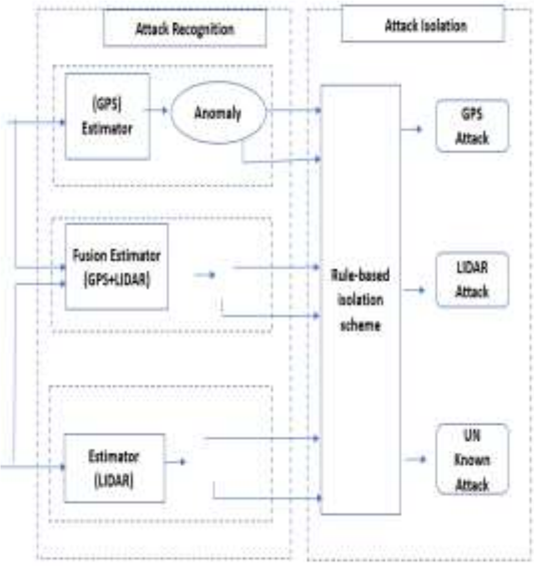
In this study, we use 10HZ GPS and LIDAR readings with actuator instructions for rate and steering angle to identify and identify sensor assaults were launched, and the GPS and LIDAR readings for location and orientation were not displayed, while commands and readings for hurry and front steering angle revealed that the vehicle's real speed while front moving angle were zero at the beginning and end of the trial, far below the corresponding directives. In this case, the discrepancy in the location readings of Satellite navigation along with LIDAR was caused by the supervisor of safety manually applying the stop button at certain times in order to ensure the health of the test, but it also rendered the proposed structure useless. The root reason is that our GPS device only provides reliable orientation observations when the car is in motion. The event also has a warm-up session during which the pace is raised progressively once it reaches the designated level.

Kalman filter : The level of safety an autonomous car provides is paramount. To guarantee the security of cars in motion while under active control, vehicles are equipped with something called a vehicle stability control system (VSC), which employs several motion parameters to determine the most suitable control approach.Numerous sensors in a car may often be employed to ascertain its current motion status. Given the current state of the art, it is either impossible or too costly to directly measure some essential characteristics, which include speed and yaw rate, making parameter estimation the preferred method for satisfying a need for a vehicle stability control system. The kalman filter method can handle this problem.The kalman determine algorithm consists of a prediction phase and an update phase in which measurements are taken. In the prediction stage, the Kalman filter produces estimates about the current state constant alongside their uncertainty.After the conclusion of the following measurement, which is always flawed by some degree of error, including accidental noise, is detected, these estimates are revised using an average with weighting, giving greater weight to guesses with higher confidence..

For clarity, let's use an example to see how the fikter may be used. When it comes to navigation and positioning, autonomous cars rely on signals are poor, we will have to rely on the IMU and odometer data instead.Using Kalman filters, we can aggregate these three measurements and estimate where the automobile is in the tunnel.

We have already discussed a linear recursive minimal-squares filter that is quite close to the Kalman filter. In contrast to recursive least squares, Kalman filter may update a figure of a dynamic state, while this is only possible for estimates of fixed parameters.by use of a dual process of forecasting and adjusting The Kalman filter attempts to update this state based on a probabilistic estimate in real time. Let's look at an issue of anticipating the vehicle's 1D location to better understand these ideas.

Block Diagram:



Results:, our team has conducted many tests utilising data collected by an autonomous vehicle. GPS and a 3D LIDAR technology are installed in the vehicle. The information was collected at the centre of excellence. A safety supervisor rode along in the vehicle while data was being collected in case of an unexpected incident. Nonetheless, the vehicle's internal sensors and awareness allowed it to navigate on its own. The vehicle used Autowave, an open-source application built on the ROS platform, to provide autonomous driving in metropolitan areas. A rosbag based on sensor readings was used to record all of the papers that included data on perception, location, planning, and control. Autowave routinely generates instructions for vehicle speed and angle of tilt while maintaining kinematic control. The low-level controller receives these directives and carries them out.

During the road experiments, the cars drove around the spot once without being attacked. Location and orientation information gathered via GPS and LIDAR.

TABLE:

PROPOSED ATTACK ISOLATION SCHEME

Case	Detector 1	Detector 2	Detector 3	Result
1	No Alarm	No Alarm	No Alarm	No Attack
2	No Alarm	No Alarm	Alarm	Unknown Attack
3	No Alarm	Alarm	No Alarm	LIDAR Attack
4	No Alarm	Alarm	Alarm	LIDAR Attack
5	Alarm	No Alarm	No Alarm	GPS Attack

6	Alarm	No Alarm	Alarm	GPS Attack
7	Alarm	Alarm	No Alarm	GPS and LIDAR Attack
8	Alarm	Alarm	Alarm	GPS and LIDAR Attack

Case 1: In this case, no detectors trigger their alarms, suggesting that the data collected by their sensors is consistent with what may be expected according to the relevant mathematical model. Since then, GPS and LIDAR have resumed their usual operations..

Case 2: Detectors 1 and 2 return a match even if neither the GPS nor the LIDAR sensor value matches the matching expectation. The lack of activity from The sensors 1 and 2 might be because the attack was so weak that it was obscured by background noise in the measuring and processing procedures. However, the gap between these two metrics widens with time, triggering the alarm in Detector 3. This might be seen as an assault, the source of which is still unclear.

Case 3: In Detector 2 raises an alarm, whereas Detectors 1 and 3 don't, since the LIDAR result is inconsistent with expectations, but the similarity between the GPS and Rgb readings is within tolerance. Detector 3 incorporates both GPS and LIDAR data into its posture estimate calculations. can happen in practise if an attacker skillfully manipulates the LIDAR measurement. If that's the case,

Case 4: When Sensor 1 is silent while The sensors 2 and 3 show anomalies, it means that LIDAR is under assault but GPS is unaffected. A alert is triggered if there is a disparity between GPS and LIDAR readings.

Case 5: Anomaly detection by Detector 1 shows that the GPS data does not conform to expectations, whereas the absence of anomaly detection by Detectors 2 and 3 suggests that the GPS and LIDAR findings are consistent and that the sensor is operating correctly. The attacker's skillful manipulation makes Case 3 a realistic possibility.

Case 6: Anomalies are picked up by Detectors 1 and 3, but not by Detector 2. Similar to the results in instance 4, it is feasible to infer that GPS is under assault.

Case 7: It is clear that both GPS et LIDAR are under assault because The sensors 1 and 2 are picking up strange behaviour while Detecting 3 is performing regularly. Possible causes of Detector 3's silence include sophisticated manipulation of sensor measures to maintain steady falsified measurements.

Case 8: All three detectors have picked up anything out of the ordinary, demonstrating that the GPS and LIDAR are both vulnerable to attack. Detector 3's abnormality is due to its inconsistent erroneous readings..

Conclusion and Future scope: As part of this study, we present a model-based method for detecting and mitigating hacks on the sensor array of autonomous cars. The information security of autonomous vehicles is considerably improved by including a network of intrusion detectors, which makes it possible to develop a rule-driven attack division system capable of detecting and identifying sensor attacks. Our proposed concept has been proven effective through experimental testing with data from actual vehicles. Attacks of the denial-of-service, lateral movement, stealth, and replay kind of the many types of attacks that have been carefully considered in developing seven different attack scenarios. The findings show that a model-based strategy to monitoring GPS signals is insufficient to avoid stealthy attacks, but that an additional detector that records inconsistencies between data from different sensors may be identified. The aforementioned flaws in the proposed method should not be overlooked. There will be initiatives implemented in the future to address these concerns.

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. Compute. Commune. Secure., Nov. 2019, pp. 2267-2281.

[3] D.Davidson, H. Wu, Jelinek, 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. DE Marinis, S. Telex, 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. Atom. (ICRA), May 2019, pp. 8514-8521.

[5] J. Petit and S.E. Shladover, “Potential cyberattacks on automated vehicles,” IEEE Trans. Intel. 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 (I Things) IEEE Green Compute. Commune. (GreenCom) IEEE Cyber, Phys. Social Compute. (CPSCom) IEEE Smart Data (Smart Data), 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. Intel. Transp. Syst., vol. 18, no. 11, pp. 2898-2915, Nov. 2017.

[8] A. 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 Compute. Commune. Int. Symp. Cyberspace Secure. (IUCC-CSS). Dec. 2016, pp. 61-68.

[9] A. Bezemskij, G. Loukas, D. Gan, and R.J. Anthony,” Detection cyber-physical threats in an autonomous robotic vehicle using Bayesian networks,” in Proc. IEEE Int. Conf. Internet Things (I THINGS) IEEE Green compute. Commune. (GreenCom) IEEE Cyber, Phys. Social Compute. (CPSCom) IEEE Smart Data (Smart Data), 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. Intel. Robots Syst. (IROS), Nov. 2019, pp. 984-989.

[11] D. Suo and S.E. Sarma, “Real-time trust-building schemes for mitigating malicious behaviours in connected and automated vehicles,” in Proc. IEEE Intel. 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 Intel. 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. Sanchez, 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] A.M. Guerrero-Higuera’s, N. DeCastro -Garcia, and V. Matellian, “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. Intel. 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. Intel. 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. Common., 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. Intel. 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. Raths, 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. Mousasi, 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. Raj Bahadur, A. J. Malton, A. Wallenstein, and A. E. Hassan, “A survey of anomaly detection for connected vehicle cybersecurity and safety,” in Proc. IEEE Intel. 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. Geraldo et al., “A survey of physics-based attack detection in cyber physical systems,” ACM Compute. Surv., vol. 51, no. 4, pp. 1–36, 2018