2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

Cyber-Physical Security for Connected and Automated Electric Vehicles

Mr.M.Sandeep kumar,M.tech(Computer Science),Student,School of Information Technology, JNTUH,Kukatpally,Hyderabad .sandeepmallurics@gmail.com

Dr.V.Uma Rani,Professor,Department of CSE,School of Information Technology, JNTUH,Kukatpally,Hyderabad. umarani_vanamala@yahoo.com.

ABSTRACT: This study proposes, for the first time to our knowledge, a thorough evaluation of the cyber-physical security of the energy management system for connected and automated electric vehicles. The created generalized technique for analyzing the effects of cyberattacks includes cutting-edge evaluation metrics for the energy management system's steady state and transient performance as well as revolutionary index-based resilience and security standards. In particular, we suggest a security criterion based on dynamic performance, comfortability, and energy, which are the most important metrics to assess an electronic control unit's (ECU) performance. An attack may be insignificant if it has no effect on these parameters. The impact of cyberattacks on ECU is thoroughly examined using the statistical findings and suggested evaluation metrics. The findings can be used as recommendations for attack detection, diagnosis, and defences.

Keywords *–Automated and connected electric vehicles, cyber–physical system, cybersecurity, impact analysis.*

1. INTRODUCTION

Vehicle-to-infrastructure/cloud-to-vehicle connections enable a large increase in the amount of traffic, road, and environmental information, which can significantly improve driving safety, comfort, and energy economy [1]. However, because there are so many embedded ECUs in networks, cybersecurity issues are also raised. The automobiles are susceptible to cyberattacks, as shown by recent incidents [2]–[4], which would enable an attacker to get around the vehicle control systems and have serious repercussions such disabling brakes, shutting off headlights, and taking control of steering. [4]–[6]. By way of illustration, hacks on antilock braking systems in [7] show how a malicious actor might alter the feedback measurements via wheel speed sensors and create potentially fatal circumstances. An autonomous vehicle may deviate from its intended trajectory as a result of spoofing attacks on the Global Positioning System [8]. A few hacks using direct (by connecting with the OBD-II port on the vehicle) and remote (via Bluetooth-enabled wireless channels) access have also been documented in the literature [4], [5], [9], and [10]. Furthermore, in the past two years, real-world scenarios have drawn more attention to and discussion of cyberattacks in

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

CAVs via vehicle-to-vehicle and vehicle-to-infrastructure channels.

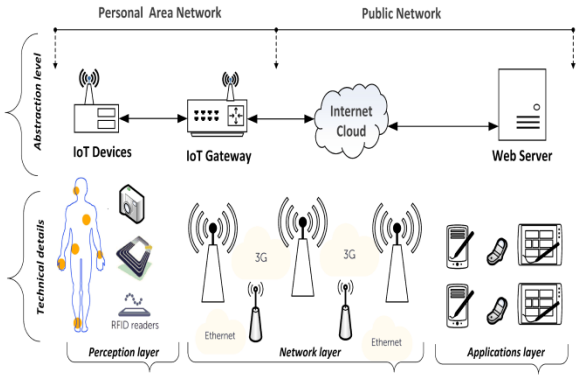

Fig.1: Cloud computing environment

In particular, compared to an internal combustion engine (ICE) vehicle, the cyber-physical security of connected and automated electric vehicles (CAEVs) is receiving much more attention due to the connection with battery charging infrastructure, more centralised control architecture, and higher electrification. For instance, the CAEVs may be vulnerable to cyberattacks due to communication between the CAEVs, charging stations, and smart grid. Because an anomalous system measurement is a clear sign of potential cyber attacks, cyber-physical security monitoring can act as an additional layer of defence in comparison to standard cyber techniques for ICE cars, which concentrate on a vehicle's entry points [5], [9]. On CAEVs, however, cyber-physical security is still in its early stages. Due to a lack of security monitoring, they are vulnerable to a variety of cyberattacks, including man-in-the-middle attacks that impair the functioning of the vehicle and traditional eavesdropping and denial of service (DOS) attacks [14]. Because they have the potential to physically harm people, vehicles, and infrastructure, the results could be disastrous (the grid). On the cyber security of battery management systems, some basic research has been done [15]–[17]. To our knowledge, however, there are no works in existence for threat-resilient control, cyber-threat detection, or vulnerability evaluation of core control units for CAEVs driven by numerous electric machines.

2. LITERATURE REVIEW

Autonomous vehicle systems within an intelligent transportation systems (ITS) paradigm have drawn steadily rising interest from both academia and the industry, according to J. K. Naufal et al. Without safety, the ideal of driverless vehicles cannot be realised. Safety is a vital feature. In order to develop and implement an autonomous supervision and control system, this study provides a novel conceptual framework, supported by a consolidated, international normative risk management procedure, and is based on a safety-critical architecture imported from an analogous transportation sector (SCS). This SCS technique, based on automotive cyber physical systems (ACPSs), is known as autonomous ACPS, and it intends to reduce risks associated with probable loss of human life in the automobile transportation sector by deploying resilient actions at run-time.

According to M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee et al., the incidence of security-related events involving control systems has significantly increased in recent years. These include high-profile attacks across a variety of

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

application domains, from attacks on critical infrastructure, as in the case of the Maroochy Water breach [1], and industrial systems, to attacks on modern vehicles [6] to [8]. Examples include the StuxNet virus attack on an industrial supervisory control and data acquisition system [2], [3], and the German Steel Mill cyberattack [4], [5]. Even very reliable military systems have been proved to be susceptible to attacks, as demonstrated by the widely reported downing of the American drone RQ-170 Sentinel [9]–[11]. The necessity for security in cyberphysical systems (CPSs), which tightly couple computation and communication substrates with sensing and actuation components, has been dramatically increased as a result of these accidents. However, the complexity and heterogeneity of the upcoming generation of networked, embedded, and safety-critical control systems have presented challenges to the established design methodologies, where security is typically conceived of as an afterthought.

Modern urban vehicles adapt sensing, communication, and computing modules into nearly every functional component to aid humans in driving, according to P. Guo, H. Kim, L. Guan, M. Zhu, and P. Liu et al. But because of their inherent vulnerability to threats, new technologies put automobiles at serious security risk. In this study, we concentrate on the identification of sensor and actuator attacks that have the potential to actively change vehicle behaviour and directly harm both people and cars. We create a cooperative intrusion detection system that uses sensing information from each vehicle's onboard sensors and nearby cars to identify sensor and actuator attacks without the need for a central authority. Clean data and contaminated data are uniquely correlated through the physical dynamics of the vehicle, which is how the detection makes use of this feature. We launch attacks across several attack channels in a scaled autonomous vehicle testbed to show the efficiency of the detection system.

According to K. Koscher et al., modern cars are much more than just mechanical machines; they are constantly being monitored and managed by dozens of digital computers that are coordinated through internal vehicle networks. While this change has led to significant improvements in safety and efficiency, it has also brought about a number of new potential concerns. We empirically assess these problems on a contemporary car in this research and show the weakness of the underlying system structure. We show that an attacker who can gain access to almost any Electronic Control Unit (ECU) can use this to entirely bypass a wide range of safety-critical systems. We demonstrate the capacity to adversarially control a variety of automotive functions and completely disregard driver input through a number of experiments, both in the lab and on the road. These include disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and more. We discover that it is possible to get over the car's basic network security measures, such as by nefariously bridging across the two internal subnets. We also describe composite assaults that take use of specific flaws, such as one that inserts

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

malicious code into a car's telematics unit and entirely wipes up any traces of its existence following a collision. Looking ahead, we explore the difficult issues in resolving these vulnerabilities while taking the current automobile environment into account.

According to S Checkoway et al., modern cars are heavily computerised and hence might be attacked. The internal networks of some modern cars have been found to be vulnerable in recent studies, but the accompanying threat model—requiring prior physical access—has rightfully been seen as unrealistic. Therefore, whether cars can also be vulnerable to remote compromise is still an unanswered subject. By methodically examining the exterior attack surface of a modern car, our work aims to put an end to this debate. We find that a variety of attack vectors, such as mechanical tools, CD players, Bluetooth, and cellular radio, make remote exploitation possible. We also find that wireless communications channels enable remote vehicle control, location tracking, in-cabin audio exfiltration, and theft. Finally, we highlight the practical difficulties in mitigating these issues and analyse the structural features of the automobile ecosystem that give birth to them.

3. IMPLEMENTATION

In the modern world, sensors are utilised everywhere to monitor. These sensors are utilised in a variety of automotive components, including the braking system, steering, tyres, and other areas that can sense data (such as slippery road conditions or approaching pedestrians) or receive commands from electronic component units (ECUs) and then act accordingly. Security issues arise because these devices can run without human oversight since a hostile attacker could acquire control of the sensors and modify their instructions. Attacker may order the sensor to perform a sudden break apply command or another erroneous instruction, endangering people's lives in the process.

A DOS (denial of service) can be caused by the attacker by submitting several requests that would otherwise be pointless and repetitive (send repeated commands again and again). Batteries are required for the operation of all sensors, and submitting frequent or large requests continuously may drain the battery faster. In order to analyse the consequences of such attacks and decrease battery consumption, the author analyses energy utilisation in a variety of attack scenarios. The author then makes the suggestion to avoid such attacks in order to save energy; this method is called Energy Management System (EMS). Model Prediction Control (MPC) is a technique for managing EMS.

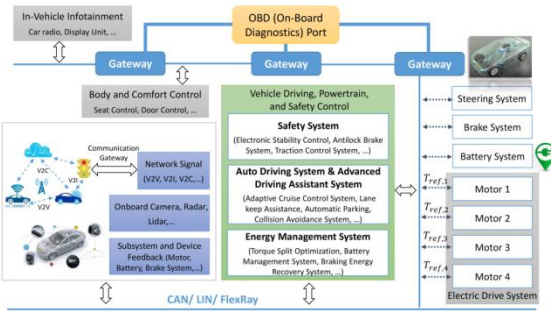

Fig.2: Smart surveillance framework.

A system-level ECU, which may be divided into three components based on their various tasks, controls a four-wheel drive CAEV, as

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

shown in Fig. 2. These parts are the safety system, EMS, and auto or auxiliary drive system. It should be noted that "EMS" in this article is a broad term that includes many efficiency-motivated control systems, for example, energy-efficient velocity profile optimization, battery management system, and braking energy recovery system, as shown in Fig. 2. In addition to energy management, which only refers to energy allocation with specific driving demands (for example, torque split in vehicles with multipower sources). These control systems, which include the steering system, electric drive system, battery, and brake system, are designed based on the superfluous intelligent information from V2X and onboard sensors. In the meantime, high-speed control area network buses, the local interconnect network, and Flexray communication are used to transport all of the signals.

The attacker's ability to reflash and rewrite all of the signals on the automotive network is assumed in this paper. After that, the effects of faulty sensing and perception of the end-goals can be examined. Generally speaking, the safety system concentrates on ensuring longitudinal and yaw stability by increasing steering or managing the brake forces. This scenario frequently happens when there are bad driving circumstances, such as a slippery road surface, emergency braking, and steering. The inputs come from the chassis sensors, such as the engine and wheel speeds, the accelerator and brake pedals, the steering angle, and feedback signals for yaw stability. Therefore, when tracking the desired course and velocity trajectory, the objectives can be described as the vehicle's yaw angle, yaw rate, and tracking error. The autodrive system (also known as an advanced driver assistance system) is created from the standpoint of a driving strategy that can aid or replace a human driver in controlling the vehicle. The steering reference and signal inputs and outputs are the same as those of an EMS. Following that, the goal is the gap in distance between the host and the nearby vehicles, tracking errors of the intended speed, acceleration, and its rate, tracking errors of the path trajectory, and the driving decision.

4. IMPLEMENTATION

According to this paper's author, connected and automatic vehicles (CAEV) are secure against cyber and physical threats. Nowadays, sensors are used everywhere for monitoring. These sensors are used inside different parts of vehicles, such as the braking system, steering, tyres, and other places that will sense data (like slippery tyres or people approaching vehicles) or receive commands from ECUs (electronic component units), and then act in response to those commands. The fact that these devices can operate without human supervision raises security concerns since a malicious attacker could seize control of the sensors and change their instructions. Attacker can instruct a sensor to apply a sudden break or do anything else odd, and the sensor's execution of such instructions will endanger the lives of people.

The attacker can cause a DOS (denial of service) by sending several requests that would otherwise be unnecessary and repetitive (send repeated commands again

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

and again). All sensors use batteries to operate, and sending frequent or large requests continually may use up more battery. Author evaluates energy usage in various attack scenarios in order to analyse the effects of such attacks and reduce battery consumption. Author then suggests avoiding such attacks in order to conserve energy, and this process is known as Energy Management System (EMS). Model Prediction Control (MPC) is a strategy that can be used to control EMS .

By subtracting the current time vehicle speed from the previous time vehicle speed, the author can predict abnormal or attack conditions. If there is a sudden change in velocity for a sustained period of time, the attack will be taken into consideration, and the system will avoid such attacks to conserve energy and wait until it receives normal commands to recover. We can reduce energy consumption and lengthen vehicle travel times by avoiding such orders.

We have created a simulation in which vehicles drive on a road in response to commands from an ECU. We then track vehicle velocity to identify normal and attack scenarios and report energy usage in both cases.

6. EXPERIMENTAL RESULTS

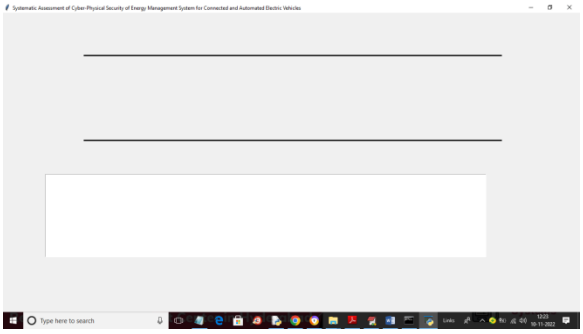

Fig.4: Output

Black lines on the screen above represent the road, and when the ECU issues commands, the vehicles will begin to move.

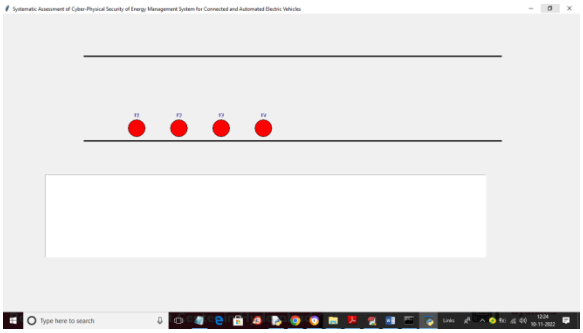

Fig.5: Output

The red circles on the screen above represent the vehicles that will continue to move in response to directives from the ECU.

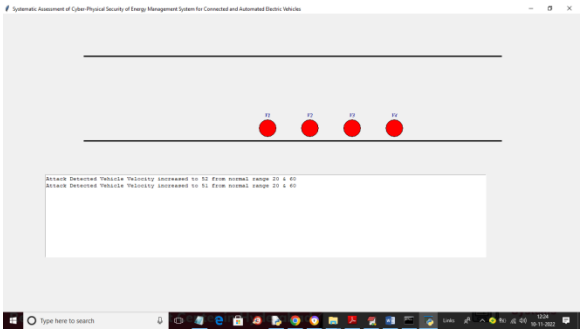

Fig.6: Output

We are showing aberrant commands received by vehicles based on velocity in the text area of the aforementioned screen. Attack will be recognized if there is a sudden shift in velocity from the normal range.

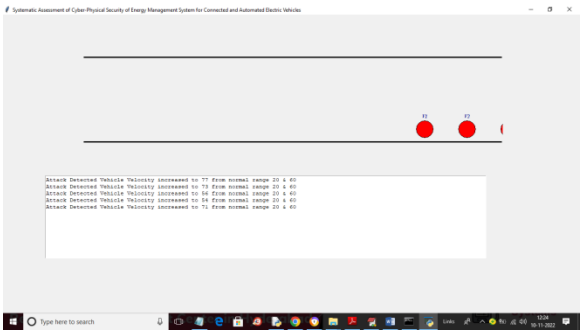

Fig.7: Output

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Vehicles are travelling in the screen above, and we can see strange commands that the vehicles have received in the text field. the graph of energy use shown below following simulation.

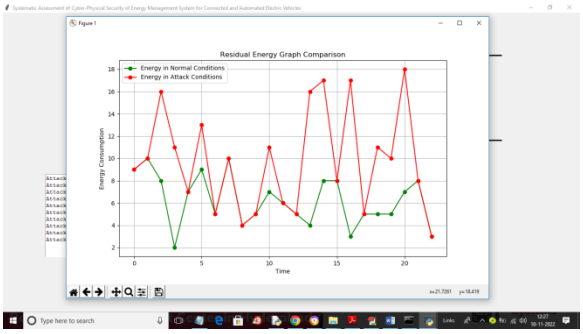

Fig.8: Output

In the graph above, the x-axis is time, the y-axis is vehicle energy consumption, and the green line shows energy consumption in non-attacking conditions while the red line shows energy consumption during an attack. So, by staying away from DOS and repeat attacks, we were able to minimise energy use to the level indicated by the green line.

6. CONCLUSION

In order to study the impact of cyberattacks on various vital systems and signals as well as the interaction between these subsystems thoroughly, this article established general guidelines for vulnerability assessment of core control systems for CAEVs. We created an MPC-based EMS for CAEVs with four in-wheel motors as a case study and provided a methodical vulnerability analysis on cyber threats. Then, novel index-based assessment criteria were developed to assess critical performance in terms of dynamic performance, comfort, energy use, and system security and resilience. We then made a few comments about practical uses and future research. In this post, we showed how data integrity assaults could allow an attacker to degrade the vehicle's overall performance by causing torque ripples and increased velocity tracking errors, decreased energy efficiency, and even instability. The results indicated that all of the evaluation metrics, including the suggested recovery time and resilience indices, could accurately depict the effects of different cyber attacks for the created MPC-based EMS. The development of data- or model-based detection and diagnosis algorithms for use in real-world applications is therefore possible employing these metrics. Additionally, the statistical findings can aid in identifying the crucial signals so that system designers can give them more consideration when creating a system. To increase the accuracy of the essential feedback measurements, you may, for instance, utilise encryption, observer, numerous signals, or contact with other control systems that can provide an approximated value. It should be mentioned that this article presents a broad framework for vulnerability evaluation of a control system in the ECU in addition to a detailed effect analysis of cyber threats on EMS (from the control perspective). For other systems, such as the advanced driver assistance and safety systems in Fig. 2, one must perform a thorough effect analysis utilising the potential signal inputs and goals listed under a variety of cyber-physical attacks in accordance with specific requirements. Although vulnerability assessment can be addressed by designing various cyber-physical attacks and evaluation metrics as described in this article, for those learning-based systems,

such as a pedestrian detection system in deep learning approaches in adverse weather, additional research is required due to the unique algorithm structure compared to conventional control methodologies.

REFERENCES

[1] J. K. Naufal et al., "A2 CPS: A vehicle-centric safety conceptual framework for autonomous transport systems," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 6, pp. 1925–1939, Jun. 2018.

[2] M. Pajic, J. Weimer, N. Bezzo, O. Sokolsky, G. J. Pappas, and I. Lee, "Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators," IEEE Control Syst. Mag., vol. 37, no. 2, pp. 66–81, Apr. 2017.

[3] P. Guo, H. Kim, L. Guan, M. Zhu, and P. Liu, "Vcids: Collaborative intrusion detection of sensor and actuator attacks on connected vehicles," in Proc. Int. Conf. Secur. Privacy Commun. Syst, 2017, pp. 377–396.

[4] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proc. IEEE Symp. Secur. Privacy, 2010, pp. 447–462.

[5] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces.," in Proc. USENIX Secur. Symp., 2011, pp. 447–462.

[6] C. Valasek and C. Miller, "Adventures in automotive networks and control units," Tech. White Paper, IOActive, 2014.

[7] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in Proc. Int. Workshop Cryptographic Hardware Embedded Syst., 2013, pp. 55–72.

[8] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in Proc. ACM Symp. Comput. Commun. Secur., 2011, pp. 75–86.

[9] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," IEEE Internet Things J., vol. 1, no. 1, pp. 10–21, Feb. 2014.

[10] GAO-16-350, "Vehicle cybersecurity dot and industry have efforts under way, but dot needs to define its role in responding to a real-world attack," US Government Accountability Office, Mar. 24, 2016.[Online]. Available: https://www.gao.gov/assets/680/676064.pdf