International Journal of Future Generation Communication and Networking
Vol.14, No. 1, (2021), pp. 4104 – 4111

Classification of Attacks On Autonomous Cars

Antariksh Pratham[1], Pramod Sonawane[2], Sneha Kamble[3], Siddhi Sali[4]

Department of Electronics and Telecommunication, Pimpri Chinchwad College of Engineering

[1]antariksh.pratham@pccoepune.org

[2]pramod.sonawane@pccoepune.org

[3]snehakamble076@gmail.com

[4]siddhisali9999@gmail.com

Abstract

Automotive manufacturers have stated that completely autonomous driving, referred to by Tesla Motors as FSD, will become a part of the market in the coming years, and by 2030. There are a lot of advantages once FSD comes out of beta into general availability. Driver-assist features have been made available for a long time and saved countless hours in driving. Such features also help people like the elderly and specially challenged groups of people who are impaired from one of their limbs and are unable to drive cars. However, there is another aspect that should not be completely ignored.

Nowadays cars are fast progressing towards completely self-driving themselves on roads, however, we also must be increasingly careful as we add more and more features to our cars. The more connected the vehicle infrastructure and onboard electronics are, the easier it becomes for someone with mala fide intentions to break in and gain access to exploit it to do things according to their own will.

The increased connectivity combined with autonomous driving functions poses a considerable threat to the vast socio-economic benefits promised by AVs. However, there is not much historical data available on autonomous driving which means that traditional methods of risk assessment become ineffective. Thus, the authors are trying to explore the security aspect of connected cars and autonomous driving technology. Through this research, they want to provide cybersecurity professionals and automakers with the tools and knowledge to identify vulnerabilities, exploits and even give recommendations for mitigating any threats to the car and onboard computing infrastructure. Anyone who is working towards making cars safer like policymakers, professionals can find our project to be extremely helpful to them for their research. The analysis has been conducted by using a prototype based on Reinforcement Learning (RL), Proximal Policy Optimisation (PPO), and Sim2Real learning.

Keywords— *AWS, Autonomous Vehicles, Cybersecurity, Cloud Computing.*

I. INTRODUCTION

With the rapid development of computer vision techniques and of technology in general, autonomous cars are inevitably going to be a reality in the years to come, as early as 2025[1]. Moore's law[2] has enabled us to innovate at an unprecedented speed which made this possible. We are very close to having self-driving autonomous cars on our roads soon, thanks to many people who have been working on various implementations of the technology[3]. People have been researching this ever since the automobile. Francis Udina demonstrated a remote controlled car, famously known as American Wonder in 1925. GM also advertised that they would bring self-driving technology to consumers as early as the 1970s. They were also among the first to make people truly understand the benefits of having

ISSN: 2233-7853 IJFGCN

autonomous driving technology. At that time it might have seemed a little optimistic, but it is incredible how many of these predictions are now becoming available in the market thanks to technology.

The autonomous driving industry is witnessing a meteoric growth and is expected to be worth billions by 2025. Gartner has even forecasted that up to 740k vehicles will be added by 2023 with fully capable self-driving hardware[4]. AVs can make the lives of people with special abilities way simpler and assist them in their day-to-day activities for which they had to be dependent on someone else. This technology will provide them with the freedom to travel independently and without any issues. 33% of drivers in the U.S. feel that semi-autonomous features in vehicles like automated park assist, lane departure sensors, and autopilot for self-driving will make them better drivers.

This dream's inspiration comes straight from the reality of driving in heavy traffic. More than 94 percent of all driving accidents today are caused by human error. In that case we could minimize or eliminate driving deaths by taking human error out of the picture through automation. Many other profound benefits could arise from a driverless future. Instead of focusing on lanes, turns, and traffic, you can reply to work emails. Eat or relax and make the morning so much more productive. We can extend the mobility the driving provides to the entire human population, not just those able to perform the driving task.

However, as we slowly head towards a driverless future with cars like Tesla[3] already advertising FSD as a worldwide Beta, with general availability expected anytime soon, we also have to keep in mind the widespread ramifications of having such advanced technology. Surely there will be a lot of ethical and technical concerns with it. There are a bunch of ethical concerns with this kind of advanced technology as well. Is it mature enough to be introduced into the market? Will it be able to deliver on the promise of drastically reducing car accidents and improving quality of driving? One of the biggest motivations behind making autonomous cars is to improve car safety and efficiency. Sebastian Thrun, the leading engineer of Google's self-driving car project Waymo, wrote in his blog that the goal of developing self-driving cars is to "help prevent traffic accidents, free up people's time and reduce carbon emissions."[5]

There is less adoption of autonomous driving technology around the world. 56% of Americans said that they would not prefer being driven around in a self-driving car. The reason for that is straight, the technology is still not there. The most advanced car in production today, the Tesla, is still categorised as a Level 2 system under SAE J3016[6]. In addition to that, Tesla has also faced flak from various sectors for not doing enough to protect the cars from accidents and blunders[7]. Most of the time they happen due to the fault of the person behind the wheel, but there should be some system to mitigate such disasters in judgement. Because of this, it is taking a long time for self-driving technology to come to the furore.

We have tried to address this issue from the perspective of protecting AVs from cyber-attacks. Our goal is to program a car for autonomous driving, and then demonstrate various security loopholes in its design and make recommendations on how to plug them. In doing so, we envision a safe and secure world for us where autonomous cars can be used without any threat of being compromised thus also jeopardising the lives of everyone who are in the car.

II. AUTONOMOUS DRIVING TECHNOLOGY

ISSN: 2233-7853 IJFGCN

We have been experimenting on Autonomous Cars for a while now and soon we will be having fully autonomous cars on our roads as well. There have been various attempts in the past at deploying such technologies for the general public with advanced features, and we are able to see the results of that now. The United States carried out the Connected Vehicle Deployment Program[8], [9] across 4 cities with an investment of $45m to assess and better understand how to implement such advanced technology.

An autonomous car, or CAV, contains several components that enable it to get a better understanding of its environment, like laser, radar, cameras, LiDAR, and various connection and networking mechanisms Bluetooth, WiFi, and Wireless Access in Vehicular Environments (WAVE)[10]. These components help the onboard computer get a sense of the environment around it and make calculated decisions to avoid obstacles and travel.

There are various levels of automation in autonomous cars, which range from no automation to full automation. SAE
publishes standards, and references for the levels of automation[6]. These five levels of automation are – Level 0 meaning no automation, Level 1 meaning most driver assistance systems, Level 2 meaning partial automation, Level 3 encompassing conditional automation, Level 4 being higher automation, and Level 5 full automation. In this paper, we mostly consider only the higher levels of automation.

III. AWS DEEP RACER

AWS DeepRacer uses Proximal Policy Optimisation (PPO)[11] method to train the Reinforcement Learning (RL) model which drives the car[12]. It is a derivative of the Policy gradient method. It works in discrete and continuous action space, which is great for our application. However, one of the key disadvantages of using PPO is that the model may sometimes stick to learned information and become even more and more certain about choosing an action. This is also known as exploitation. In order to avoid this from happening, we have used entropy regularization to encourage the model to explore more in the action space.

PPO works by making the agent search for the optimal policy #* ($a \mid s$; #*). In order to learn the optimal policy, the agent goes through an iterative process of trial and error. The agent takes a random initial action to arrive at a new state. It then iterates from that step to the new one. This interaction of the agent from an initial to a terminal state is called an episode. The optimal policy is learned by using this iterative approach for each episode (s, a, r), each time adding some more learning to older learned models. The overall probability ratio between the old and new models learned by the PPO algorithm is denoted by

$$r(\theta) = \frac{\pi_\theta(s)}{\pi_{\theta_{old}}(s)}$$

Over time, the agent comes to know which actions lead to long-term rewards and is thus able to learn the optimal policy.

$$\theta_{\tau+1} = \theta_\tau + \alpha \nabla_\theta J(\theta)$$

ISSN: 2233-7853 IJFGCN

The goal of optimisation is to try and maximise the policy score function $J(\#)$. The policy score function represents the immediate reward $r(\ s\ ,a\ )$ in a given action (a) and space (s) averaged over state probability distribution $\#(\ s\ )$ and the action probability distribution (# ($a \mid s$; #)):

$$J(\theta) = \sum_{s \in S} \rho(s) \sum_{a \in A} \pi(s;\theta) r(s,a)$$

The maximisation proceeds by following the policy gradient ascent over the episodes of training data (s, a, r):

This can also be represented in terms of the future reward as:

$$R(\tau) = R(s_\tau, r_\tau) = \sum_{t=0}^{H} \gamma^t r(s_{\tau+1}, r_{\tau+1})$$

Where γ is the discount factor ranging from 0 to 1, and τ maps to an experience (s_τ, a_τ, r_τ) at step τ and the summation includes experiences ranging from t = 0 to t = H when the agent goes off-track or reaches the finish line.

Also, the loss function for value network weights is:

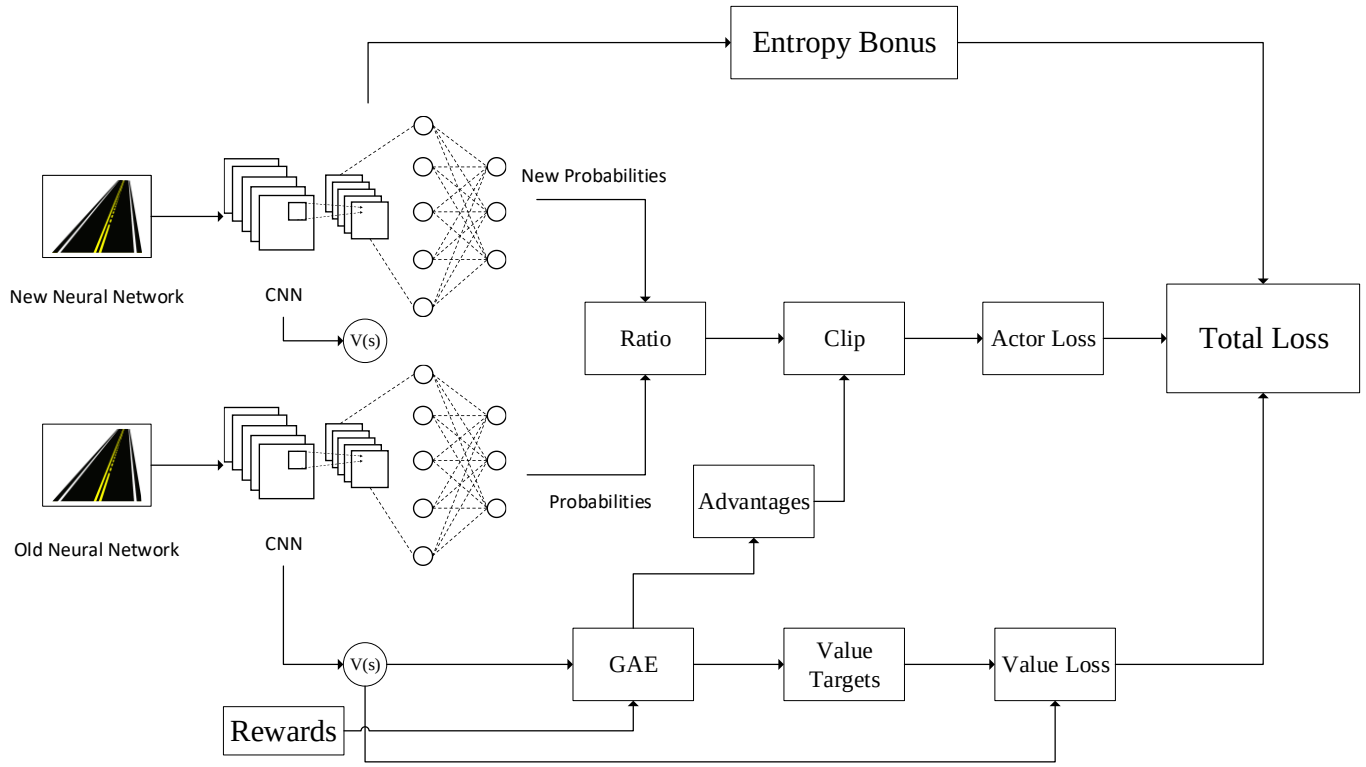
$$L(\phi) = \frac{1}{2} \sum_{i,t} \left(V_\phi(s_{i,t}) - y_{i,t}\right)^2$$

Using these estimated values, the policy gradient for updating the policy network weights # is:

$$\nabla_\theta J(\theta_\tau) \approx \frac{1}{N} \sum_{i=1}^{N} \sum_{t=1}^{H} \nabla_\theta \, log \, log \left(\pi(s_{i,t};\theta)\right) \left(r(a_{i,t}, s_{i,t}) + \gamma V_\phi(s_{i,t+1}) - V_\phi(s_{i,t})\right)$$

As said earlier, the RL algorithm needs to balance exploration and exploitation in order to train the network successfully. The agent needs to explore the state and action space and identify which actions are associated with high rewards in unexplored action space. The policy network outputs the probability of taking each action and during training each action is chosen by sampling the probability distribution. In order to achieve this, PPO uses importance sampling with clipping, adding a Gaussian-Markov noise to encourage exploration and generalized advantage estimation.

ISSN: 2233-7853 IJFGCN



IV. ATTACK METHODOLOGIES

There are various commonly known attacks that can be easily ported and adapted for an embedded environment. With

a few changes, you can easily compromise connected cars remotely. Car manufactures need to have an

understanding of the security aspect of these connected and autonomous cars. Even though there haven't been any

significant attacks on autonomous cars that caused loss of life, researchers have found very serious loopholes from time

to time[13]. The problem with autonomous cars is that in the event of a compromise, there is a good chance the driver

is not in a position mentally or physically to take control and initiate immediate corrective action due to the nature of

the technology. Researchers have suggested several attacks as well as countermeasures against them highlighting their

impact on the infrastructure. They have identified issues with the sensors, ECUs, and even the network

topologies and infrastructure being used, sometimes finding vulnerabilities in production cars as well.[14], [15]

Attack models have been demonstrated on various components such as GPS and LiDAR spoofing and

adversarial attacks on the camera systems

Take the camera for example. Now, the camera is an important aspect of autonomous cars. It helps them with things

ISSN: 2233-7853 IJFGCN

such as traffic sign recognition and lane detection. It also provides inputs to Deep Learning models that are deployed in cars to help them drive autonomously. Manufacturers have also tried to replace LiDAR with cameras because it is low cost[3] and we have massive computational algorithms today which can help us cut the high cost of LiDAR. However, cameras can't perform better in tricky situations like rain, fog, or snow. A simple, quick burst of 650 nm laser is enough to blind the camera rendering it almost completely useless and cause irrecoverable damage.[16]

V. Effective countermeasures

It is also important for us to understand that most of the attacks that we explored can be defended quite easily and without much effort. Thanks to the efforts of researchers in this domain, we know about some of the countermeasures that can be adopted so that cars can be made safer for the average consumers and they are not at risk from hackers and people looking to exploit connected cars. One of the most effective strategies can be to educate the people about the technology, as well as inform them about advantages and disadvantages. This by far will be the greatest investment any one company can do for it's consumers as they can better understand autonomous driving and understand their responsibility behind using such technology.This will not only defend against attacks but also help in increasing confidence. Cho. et al (2016)[17] proposed clock-based IDS which measures the clock skew of ECUs and then uses this information to fingerprint the ECUs, thus preventing them from getting tampered with. Intrusions are detected by checking for an abnormal shift in the clock skews. Encryption can also be used where it is currently not implemented, like CAN bus and signals sent by sensors[18]–[20]. Several researchers have published techniques that can be adopted for such signals. A decentralised public key infrastructure (PKI) can also help secure V2V and V2I communications [21].

VI. Conclusion

We have understood from our research about the various ways we can evaluate self driving technology. We have got an understanding of different attacks and the impact of such attacks on the car. There is a need for us to make technology that is safe in the true sense and holistically. Although a considerable amount of work has been done to make autonomous cars safer,we need to see that these frameworks are properly implemented. That is why we hope this research will be instrumental for car manufacturers and stakeholders in making connected mobility safer by designing and implementing state-of-the-art mitigation and defence strategies. Safety and security should be the basis of designing for the connected future for everyone to feel trustworthy with their electronics which would have more than surrounded them. It should be important for us to build redundancies and important measures should be taken so that in the event of a compromise, immediate and defensive mechanisms can be quickly deployed, thus saving valuable lives. Without it, with the rate at which innovation is progressing, we will only be digging our own hole.

References

ISSN: 2233-7853 IJFGCN

[1] Z. Kanter, "How Uber's Autonomous Cars Will Destroy 10 Million Jobs and Reshape the Economy by 2025," *Zack's Notes*, 2015. https://zackkanter.com/2015/01/23/how-ubers-autonomous-cars-will-destroy-10-million-jobs-by-2025/

[2] G. E. Moore, "Progress in Digital Integrated Electronics." IEEE, 1975. [Online]. Available: http://ai.eecs.umich.edu/people/conway/VLSI/BackgroundContext/SMErpt/AppB.pdf

[3] S. Ingle and M. Phute, "Tesla Autopilot : Semi Autonomous Driving, an Uptick for Future Autonomy," *International Research Journal of Engineering and Technology*, vol. 3, no. 9, pp. 369–372, 2016, [Online]. Available: www.irjet.net

[4] M. Rimol, "Gartner Forecasts More Than 740,000 Autonomous-Ready Vehicles to Be Added to Global Market in 2023," 2019. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-11-14-gartner-forecasts-more-than-740000-autonomous-ready-vehicles-to-be-added-to-global-market-in-2023

[5] S. Thrun, "What we're driving at," *Google Blog*, 2010. https://googleblog.blogspot.com/2010/10/what-were-driving-at.html (accessed Dec. 10, 2020).

[6] SAE International, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," 2018. https://www.sae.org/standards/content/j3016_201806/

[7] Crash Research & Analysis Inc., "Special Crash Investigations: On-Site Automated Driver Assistance System Crash Investigation of the 2015 Tesla Model S 70D," Washington DC, 2018.

[8] S. Z. D. Gopalakrishna, V. Garcia, A. Ragan, T. English and E. H. R. Young, M. Ahmed, F. Kitchener, N. U. Serulle, "Connected vehicle pilot deployment program phase 1, concept of operations (ConOps), ICF/Wyoming," 2015.

[9] A. R. F. Kitchener, T. English, D. Gopalakrishna, V. Garcia and N. U. S. R. Young, M. Ahmed, D. Stephens, "Connected vehicle pilot deployment program phase 2, data management plan wyoming," 2017.

[10] IEEE Standards Association, "IEEE Standard for Information Technology-Local and Metropolitan Area Networks-Specific Requirements-part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, 2010.

[11] AWS, *AWS DeepRacer Documentation*. 2019.

[12] B. Balaji *et al.*, "DeepRacer : Educational Autonomous Racing Platform for Experimentation with Sim2Real Reinforcement Learning".

[13] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015, doi: 10.1109/TITS.2014.2342271.

[14] Regulus Cyber LTD, "Tesla model 3 spoofed off the highway – regulus navigation system hack causes car to turn on its own." https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-researches-hack-navigation-system-causing-car-to-steer-off-road (accessed Jul. 11, 2020).

[15] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," 2016.

[16] M. Pham and K. Xiong, "A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles," pp. 1–24, 2020, [Online]. Available: http://arxiv.org/abs/2007.08041

[17] K. T. C. and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *25th USENIX Security Symposium*, 2016, pp. 911–927.

[18] A. van Herrewege, D. Singelee, and I. Verbauwhede, "CANAuth- a simple, backward compatible broadcast authentication protocol for CAN bus," in *ECRYPT Workshop on Lightweight Cryptograph*, 2011.

ISSN: 2233-7853 IJFGCN

[19] J. Halabi and H. Artail, "A lightweight synchronous cryptographic hash chain solution to securing the vehicle can bus," in *IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, IEEE, 2018, pp. 1–6.

[20] O. Avatefipour *et al.*, "An Intelligent Secured Framework for Cyberattack Detection in Electric Vehicles ' CAN Bus Using Machine Learning," *IEEE Access*, vol. PP, p. 1, 2019, doi: 10.1109/ACCESS.2019.2937576.

[21] R. W. van der Heijden, S. Dietzel, T. Leinmuller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," in *IEEE Communications Surveys & Tutorials*, Vol. 21., IEEE, 2018, pp. 779–811.

ISSN: 2233-7853 IJFGCN