Autonomous Vehicle Security

Abhay Singh Khanka (18309999)

***Abstract*—The rapid development of artificial intelligence has been beneficial to many fields, one of those being transportation. Vehicles are now evolving with "driver-less" automobiles, also known as autonomous vehicles, and are being introduced in the market for both civilian and military usage. With this evolution, there also arise a number of risks in security of both the vehicle and the passenger. In this paper, we will go over the usage of artificial intelligence in the automotive industry, specifically in the civilian market. Moreover, we will address security threats and identify the technical challenges and core issues of securing autonomous vehicles.**

I. Introduction

In the present era, autonomous vehicle are one of the most intriguing developments in the automotive industry as well as in the artificial intelligence field. The level of autonomy in these unmanned automated vehicles ranges from way-point navigation, trajectory tracking for detecting potential car crashes and in some cases even fully autonomous navigation. These developments have helped improve driving performance and reduced the number of driving related crashes while simultaneously giving feedback that will help improve the AI behind these vehicles.

However with the increase in autonomy of a vehicle, the risk to the security of the vehicle also increases. In this paper, we will go over the background of implementation of AI in vehicles and modern day uses as well as security challenges faced by this technology. Furthermore we will discuss the technologies behind the current security architectures as discussed in [2].

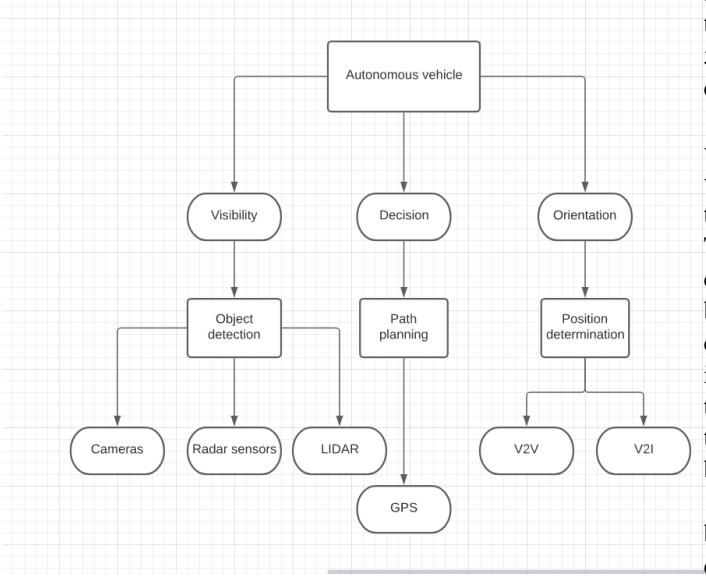

Figure 1: Elements of an Autonomous vehicle

II. Background

In the following two subsections we will be discussing applications of AI in the modern day automotive industry and also take a look at the benefits and some drawbacks of these applications. Understanding the applications and usage is crucial in determining why the safety of these autonomous vehicles is important.

A. Applications of AI in automotive industry

According to [1], there are three main applications of artificial intelligence in vehicles. We will take a look at these as follows.

1) Vehicle to everything (V2X): V2X is a vehicular technology system that enables vehicles to communicate with the traffic and the environment around them using short-range wireless signals. This communication system is mainly used for the purpose of increasing safety and preventing collisions. In a traditional vehicle, a V2X system can fetch important information regarding weather, nearby road accidents and conditions or tracking trajectories of surrounding vehicles in order to predict any accidents [1]. In addition to the aforementioned features, a V2X system in an autonomous vehicle is further capable of providing other extra information to the vehicles navigation features.

The V2X system along with the implementation of AI, has a lot of potential in making the vehicle safer and in achieving full autonomous mobility. Furthermore, its' subsets include vehicle to vehicle communication (V2V) and vehicle to infrastructure (V2I) systems all of which contribute to providing a safer experience for the inhabitants of the vehicle. This technology is currently being developed and improved by the 5G automotive association which consists of top automotive companies like BMW and Audi.

2) Vehicle control system: The application of AI in a vehicle control system is primarily to ensure the safety of the vehicle. These programs are capable of many safety measures to protect the driver from potential accidents and crashes. These techniques entail the scanning of their environment and calculating several important factors including the distance between the vehicle and the surrounding objects as well as calculating the relative velocities. Using this data a danger index is calculated and the AI program can accordingly change the velocity of the vehicle to avoid potential crashes based on the danger index. Thus the security of a vehicle is guaranteed by the application of AI in the vehicle control system.

3) Diagnostic device: In order to prevent accidents caused by faulty parts or poor maintenance, an AI powered diagnostic device is used. This device centrally controls the inner electric equipment of a vehicle uses a special CPU that diagnoses

any malfunctions in the vehicle and report them back to the driver in real time [1]. This device is used to report the state of the vehicle's equipment and identify the malfunctioning parts, thus helping to make car repair time shorter and much more cost effective for people who are inexperienced with the functioning of vehicles. Moreover, with heavy research in AI this device will even be able to predict mechanical issues before they arise thus reducing potential accidents and increasing safety of the occupants.

B. Benefits and drawbacks of Autonomous vehicles

The introduction of autonomous vehicles has a lot of potential benefits to its users and even has an impact on other people outside the vehicle as well. We will discuss all of this in detail below.

1) Benefits: Autonomous vehicles can majorly help in reducing accidents and crash risks. With the introduction of the aforementioned technologies, AVs have major potential in reducing high risk driving from inexperienced and clumsy drivers as well as support mobility for non drivers. They even help people with disabilities who usually have to spend a lot of time and money to modify their cars just to be able to drive. Furthermore, they are able to reduce stress among long distance and inexperienced drivers thus reducing risk of accidents caused by fatigue.

Autonomous vehicles have even more benefits in external factors, such as with the help of V2X technology these vehicles are capable of reducing congestion and traffic on roads. It further helps their cause that with an AI enabled vehicle control system, there is a possibility of an increase in fuel efficiency thus helping in reducing energy consumption and toxic emissions making AVs much more suitable for the environment. Reference [3] estimates that these vehicles will most likely be run on electric batteries which will have low fuel costs and would not have to pay taxes on fuel, an advantage over traditional cars which future user would certainly consider.

2) Drawbacks: In today's world, autonomous vehicles are a relatively new invention with only a few companies such as Tesla actively producing such vehicles while other companies, like Apple and Google are researching and planning to develop their own. This means that for now and for some considerable time in the near future, AVs are going to be expensive and realistically not affordable for the average person due to their high equipment and service fees. Reference [3] states that realistically these vehicles will be safe and reliable for consumer level mass production by the 2030s and affordable to the average person by the 2040s.

As of now, the security systems for these vehicles have not been proven to be completely reliable. There are still some risks of hacking and data breaches as well as the potential abuses of the features of location tracking and data collection. Since the AI behind this technology is quite dependent on data, there is always the question of how much data sharing is going on behind the surface of these vehicles and whether or not this data collection breaches any GD PR laws or other ethical concerns.

Another critical issue is that with the mass usage of these vehicles, they have the potential to lead a decline in the taxi driver industry, which could have a big impact on the lives of a lot of people.

All the above mentioned points gives the potential for AVs to be very useful in future transportation, hence it is of paramount importance that these vehicles are safe for their users as well as the environment in which they operate. We will now take a look at such safety issues

III. Security Concerns

In this section, we will go over various security threats and points of attacks of autonomous vehicles and talk of some examples of such attacks.

A. Cyber attacks

A cyber attack is an offensive type of attack targeted at digital information system, infrastructures or computer networks in order to gain or manipulate information. The threat of these attacks plays a major role in the development of security systems of autonomous vehicles. We will take a look at some of the types of cyber attacks that can take place on various components of an autonomous vehicle as talked about in reference [4].

1) Attack on camera and sensor networks: Autonomous vehicles are able to function smoothly much because of the functioning of their sensors. They are able to gather data of the surrounding environment with the help of these sensors and then pass on the data to algorithms that interpret this data and generate commands for the vehicle to follow a path or change direction accordingly. These sensors are vulnerable to external attacks and are a gateway of gaining more access to the vehicle and can possibly be manipulated in order to feed false information to the vehicle. Meanwhile, the usage of cameras in AVs is in combination with these sensors, with the camera tracking and detecting objects and traffic signs. An attack on the camera can hide particular information or objects from the view essentially leaving the vehicle running blind.

2) Attack on GPS: An autonomous vehicle navigates with the help of a global positioning system (GPS), which uses real time geographical data received from various satellites. The data is transmitted in coarse/acquisition (C/A) code which is a form of un-encrypted navigation data. It repeats every 1023 bits and modulates at a 1MHz rate with each satellite having their own unique code. This C/A code is the basis for civilian GPS use. However this does not mean that this it is safe from attacks. Even though there are more GPS' for civilian use, the technology was developed by the department of defense of the USA for military purposes. This means that the military gains access to a much more exclusive and better encrypted defense code. This code has ten times the frequency of the civilian C/A code and thus as a result is much harder to jam [5].

However, a modern day civilian use autonomous vehicle like a Tesla will not have the military level encryption making

it vulnerable to two types of GPS attacks. The first one, namely GPS jamming, results in users losing GPS location and related information. An attacker can use a software-defined radio and send out higher power broadcasts of distortion using the same GPS radio frequency. The GPS receiver locks on to this distorted signal and loses its correct position and timing. This is why the military uses much higher frequencies on their GPS'. Secondly, a GPS spoofing attack can result in inaccurate location and other information that is received by the vehicle. The methodology of this attack is very similar to the jamming attack. The attacker would use the frequency similar to the GPS with seemingly legit information and timing. Then the attacker would slowly increase the strength of the signal eventually leading to an inaccurate location in the GPS. This attack is much more complicated than the jamming attack [4].

B. Physical access

In this section we will go through some possible security concerns that would require a physical access to the vehicle. Reference [6] goes through these attacks as well as the taxonomy of attacks over vehicles.

1) Side channel attacks: A side channel attack is any attack that is based on information gained from the implementation of a computer system rather than a weakness in its structure. These types of attacks require close proximity to the vehicle and are usually non invasive in nature, with their primary aim being capturing and analysing information leaked from an autonomous vehicle.

2) Code modification and injection: An attacker is able to access the diagnosis system of an AV using an OBD-II device. This device is an inexpensive tool which is widely available in the market. This tool, originally used to perform a diagnosis on the vehicle, can be used by an attacker to access the digital infrastructure inside an AV. From here on the attacker is able to make malicious modifications to the parts of the AV such as the electronic control unit, which is basically the heart of the "Autonomous" portion of the vehicle. These malicious injections can include Trojan horses, viruses and spyware which can seriously threaten the safety of the user and the vehicle as well as vehicles and infrastructure around it. A basic defense against such attacks is to make sure all the connections to the vehicles are password protected and to have an intrusion detection system so as even if the safety of the vehicle is compromised, at least the user will know of it.

3) Packet sniffing and fuzzing: A packet analyser, or also known as packet sniffer is a software program used to intercept and log traffic that passes through a computer network. It is commonly used to diagnose network related problems by enabling the viewing of communication between a number of nodes. This program can be used by an attacker to eavesdrop on unencrypted data and collect vital information. To prevent such attacks, one must encrypt the packets that are transferred between nodes.

In a fuzzing attack, the attacker can use a program similar to that of sniffing however with the difference being that in fuzzing the data packets can be changed to show faulty values. When the faulty data packets reach the destination node, they can possibly trigger various error conditions built into the software leading the system exploitable to even worse attacks. At the same time fuzzing can be used to test security systems by deliberately sending false or invalid packets to the nodes and checking if the erroneous packets have been handled correctly or not. To defend against such attacks, the security system of the vehicle needs to be updated regularly [6].

C. Jamming attack

Jamming attacks are attacks against the external sensors, cameras and wireless networks that run in the Autonomous vehicles. These attacks are different from cyber attacks in the way that, jamming attacks directly hamper the functioning of the external sensors and networks through usually physical actions such as shining bright light into the sensor to hamper their working or jamming the signals running through an autonomous vehicle using a signal jammer. Reference [7] conducts such experiments on the sensors of autonomous vehicles.

D. Some examples of attacks

In some cases, as discussed in reference [8], the malicious modification of data packets can lead to an autonomous vehicle being unable to engage its safety related networks whereby attackers forced a fed wrong information to a vehicle by directing it to speed up in an area where there was heavy congestion thus causing an accident.

Furthermore, reference [8] discusses researchers attempting to hack into a Jeep Cherokee by exploiting an internal software vulnerability through a simple 3G connection. This technology is fairly simple and outdated however it is still able to cause such huge security breaches in an autonomous vehicle. The issue has since been fixed but it showed the vulnerability of autonomous vehicles to such attacks.

IV. Security system

In this section, we will talk about the ways the defense systems of autonomous vehicles are built as discussed in [6].

A. Securing the ECU

As mentioned previously, the electronic control unit (ECU) is one of the most important components of a vehicle, being responsible for the proper function of the unit it is controlling. ECUs are at the heart of the automotive security challenge because they and the buses that connect them need to be secured. Reference [9] proposes three types of data management systems to help better functioning as well as improved safety for the ECUs. The first of this involves having a central driving monitoring system relying on a single ECU. The proposed system is a simple one with easier management and handling. However due to only having one ECU there is a problem of having bottleneck issues for complex systems. The second type involves having a distributed data management system (DMS) which would work with multiple ECUs. This system thus reverses the pros and cons of the previous one. Finally,

the last system is a hybrid DMS consisting of a single DMS on each sub network of the vehicle.

For further security, reference [9] suggests the CAN-Auth authentication protocol for communication within the vehicle thus ensuring safety from any low to mid level attack. A downside of this system is that the CAN message has a limited size payload thus making it difficult to implement in a complex system.

B. Vehicle network security

Most modern day vehicles have in built entertainment systems that involve the usage of Bluetooth and other in-vehicle networks. These systems open up a whole new route of access for attackers to take advantage of vulnerabilities in these networks and the software inside these systems. Due to this reason, there is a need for protection of the connection between the vehicle's network and the user. Reference [10] further discusses security architectures for such networks, especially the VANET(vehicle ad-hoc) network. The author lists a number of security constraints involving the VANET network. These include issues such as network size and dynamic topology since network size can be geographically unbounded. Some further issues concern the high dependence of security mechanisms on key distribution and challenging forwarding algorithms.

C. Attack prevention methods

As discussed in [6], there are several methods one can employ to prevent attacks on a low to medium threat. First and foremost, a firewall needs to be in-place that would be able to regulate network traffic and keep out any intruders. This will be very important in the case for V2X technologies where a firewall can keep out any unauthorised access to the vehicle. Reference [9] further discusses a firewall and a security mechanism based on a hardware system to protect against vehicle-borne cyber security threats.

Secondly, the inner vehicular data transfer networks should be encrypted so as to prevent any tampering or fuzzing of data packets. Finally, there should be complex multiple layers of security and authentication for the user such as bio-metric identification over the vehicle and the ECU as well. These methods can ensure the vehicle can establish preventive measures.

D. Intrusion detection

Intrusion detection system is a cyber security method used to detect an attack on the communication components of a system. For autonomous vehicles that use V2X technology, this system is crucial for its security. The goal of an intrusion detection system is mainly to detect attack behaviours and analyse network traffic for any abnormal behaviour. With the help of AI this system can be improved to actively look for any weaknesses in the system and identify the faults of the system administrator and any abnormal activities which can occur due to a breach in security. Reference [11] further discusses the possibility of an automated secure cloud service framework for autonomous vehicles as well as an hybrid intrusion detection system that is based on monitoring using the deep belief network.

E. Machine learning and big data

Machine learning models can be applied to autonomous vehicles to improve their security networks. The first step to this involves collecting and storing the right data. If a car's internal network is tracked with a platform that can store and analyze reports, the vehicle can track suspicious behavior and deter attacks, or at the very least, warn drivers and minimize the effects. Once we have the correct data, we can use an attack detection model, with the help of machine learning, which is capable of analyzing signals and other data received through external ports or an internet connection to detect malware intrusions or unusual behaviour of the vehicle. Once an anomaly is detected, the model can trigger two actions. It could try and prevent the attack by telling the car to ignore the malicious commands and further block the source of the anomalies or it could alert the driver in real time and allow manual control over the vehicle.

V. CONCLUSION

Autonomous vehicles are still a fairly recent invention with rapid strides being made into further developing this technology and especially in its security to readily make it available and affordable for the general market. There are still considerable security threats to these vehicles, however most of those can be prevented with basic knowledge of prevention systems such as password protection, firewall and the other methods discussed. Furthermore we discussed various attack vectors, targets and consequences in autonomous vehicles which can help users in securing their vehicles.

However, given the sheer amount of petrol or diesel run vehicles today it is unlikely that we will be seeing autonomous vehicles outnumber conventional vehicles any time in the near future. Despite that, the future of autonomous vehicles looks promising which is observable in the commitments of multi national companies like Google, Apple and Tesla to further develop and produce this technology.

In summary, we introduced the concept of AVs and the technologies behind such vehicles. We further discussed a range of various attacks on these vehicles and went over the defensive taxonomy of these vehicles. We expanded our knowledge about the potential security threats to these vehicles and how to use emerging technology to build various defensive approaches to make the AVs more secure.

REFERENCES

[1] H. Wei, "Analysis on the Applications of AI in Vehicles and the Expectation for Future," 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT), 2020, pp. 502-505, doi: 10.1109/ISCTT51595.2020.00095.

[2] A. Sui and G. Muehl, "Security for Autonomous Vehicle Networks," 2020 IEEE 3rd International Conference on Electronic Information and Communication Technology (ICEICT), 2020, pp. 67-69, doi: 10.1109/ICEICT51264.2020.9334354.

[3] Litman, T. (2020). Autonomous vehicle implementation predictions: Implications for transport planning.

[4] Raiyn, J. (2018). Data and cyber security in autonomous vehicle networks. Transport and Telecommunication, 19(4), 325-334.
[5] W. Rahiman and Z. Zainal, "An overview of development GPS navigation for autonomous car," 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA), 2013, pp. 1112-1118, doi: 10.1109/ICIEA.2013.6566533.
[6] Thing, V. L., Wu, J. (2016, December). Autonomous vehicle security: A taxonomy of attacks and defences. In 2016 ieee international conference on internet of things (ithings) and ieee green computing and communications (greencom) and ieee cyber, physical and social computing (cpscom) and ieee smart data (smartdata) (pp. 164-170). IEEE.
[7] Petit, J., Stottelaar, B., Feiri, M. (2015). Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR.
[8] S. Tout, M. Abualkibash and P. Patil, "Emerging Research in the Security of Modern and Autonomous Vehicles," 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018, pp. 0543-0547, doi: 10.1109/EIT.2018.8500204.
[9] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, Huy Kang Kim, Cybersecurity for autonomous vehicles: Review of attacks and defense, Computers Security, Volume 103, 2021,102150, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102150.
[10] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, Anis Laouiti, VANet security challenges and solutions: A survey, Vehicular Communications, Volume 7, 2017, Pages 7-20, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2017.01.002.
[11] Kang M-J, Kang J-W (2016) Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. PLoS ONE 11(6): e0155781. https://doi.org/10.1371/journal.pone.0155781