Building safer autonomous vehicles

Samy Harras
June 17, 2023

***Abstract*— The demand for autonomous vehicles is continuously rising in the automobile industry. However, the risk associated with these vehicles is currently too high to allow their marketization. The goal of this paper is to compare three promising solutions: redundant safety systems, high-precision maps, and communication protocols. This comparison is made based on three criteria: effectiveness, feasibility, and cybersecurity. Based on these criteria, communication protocols come as the best solution out of the three as it is an efficient method that comes at a relatively low-cost and above all is safe from most vicious cyber attacks. Implementing this solution will open a new market for automobiles and create more opportunities for development for the industry.**

Keywords—Autonomous vehicles, safety, safety systems, high-precision maps, communication protocols, cybersecurity.

I. Introduction

Autonomous vehicles or self-driving vehicles were an idea that emerged from the previous century. They have known an immense development during the last decade. Their focus is to improve transport services in two main ways: safety and efficiency. In their current state, autonomous vehicles are far from being perfect nor safe. It has been reported by the DMV that "434 collision reports involving autonomous vehicles, including accidents where vehicles are in autonomous mode or conventional mode" [1:1]. The issue lies in the lack of enough developed technology that could provide low-risk errors of danger assessment. Marketizing autonomous vehicles in an early stage where they are not yet fully safe could cause the production of unsatisfactory and consequently dangerous products, harmful to the public. This paper compares three possible solutions to solve this issue: redundant safety systems, high-precision maps, and communication protocols. By comparing the solutions proposed based on effectiveness, feasibility, and cybersecurity, it appears that communication protocols are the most potent solution to achieve higher safety levels in autonomous vehicles.

II. Background

The idea of self-driving vehicles has been around for about a century now, yet their presence in the car market is limited to only few brands and models and operate in a limited scope with very few real automatic features. Autonomous vehicles have been a highly researched during the last decade and immense developments were made in the field. Society of Automotive Engineering divided them into five categories by the going from level 0, where only warnings are issued, to level 5, where the vehicle has full autonomy over itself [2].

A. Problem

Current prototypes show great promise but still lack consistent danger assessment. Autonomous vehicles fail to assess obstacles and take the necessary steps to avoid them [3]. The main cause of this problem is the absence of proficient technology that could analyze and assess situation fast enough to react to emergencies. Moreover, autonomous vehicles are highly susceptible to cyber-attacks of one or more communication layers. By having different communication methods going from communication within the vehicle to long-range communication, Autonomous vehicles fall susceptible to vicious cybernetic attacks and therefore present a high danger to users and their surroundings.

B. Solutions

Redundant safety systems consist of backup sensors and cameras that ensure the detection of potential hazards if the main system fails to. This can only be done by implementing extremely reliable sensors that promptly communicate surroundings and unexpected danger. Sensor radars, cameras and LiDAR play a vital role in these types of safety systems, which makes them the core of this solution [4]. They serve as both sensors and in-vehicle communicators by both capturing environmental surroundings and communicating them to the main computer of the vehicle.

High-precision maps are maps derived from the Global Navigation Satellite Systems (GNSS). They feature high precision schemes of roads and other transportation routes that include itineraries, state of roads and traffic, and environmental hazards that could affect vehicles. As shown in fig. 1, implementing observation space representation (OSR) with real time kinematic (RTK) and state space representation (SSR) with precise point positioning (PPP), a GNSS can deliver meter level absolute positioning to even decimeter or centimeter levels of positioning [5]. Such precision allows vehicles to precisely pinpoint themselves and their surroundings and lowers the chances of accidents.

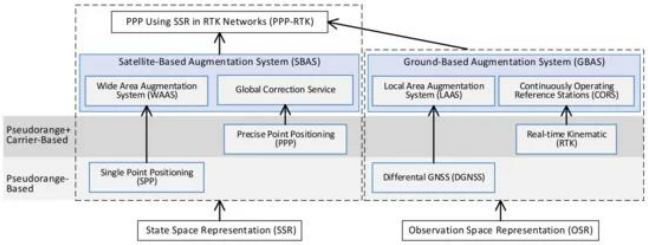

Fig. 1. GNSS positioning technology routes and development[5]

Communication protocols are communication methods within the vehicle and between other vehicles and surroundings. They exchange information between vehicles and infrastructures by using vehicle-to-vehicle signals (V2V) or vehicles-to-infrastructure signals (V2I) as shown in fig. 2. Implementation of more efficient communication protocols will lead to reducing the risk associated with communication errors. Not only that but by encrypting V2V communications, more optimal inter-vehicle communication is achieved. This allows vehicles to assess the correctness of the information it is provided in case of bugs or issues from other surrounding vehicles [6].

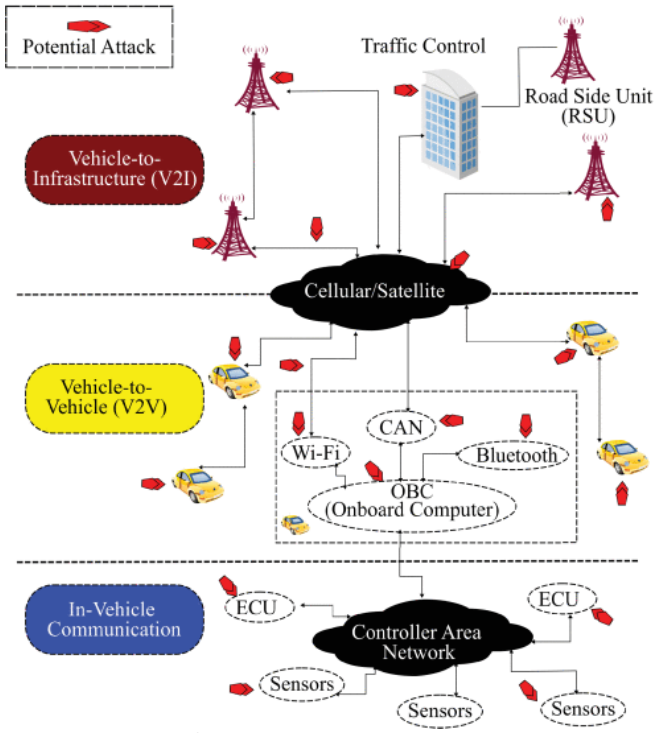

Fig. 2. Attack surfaces [3]

C. *Criteria*

The three proposed solutions will be analyzed in this paper based on three criteria: effectiveness, feasibility, and cybersecurity.

The first criterion measures the efficiency of the methods based on the rate of accidents; a percentage that shows how much risk is associated with the method studied. This criterion is critical to the matter in hand as it measures the main goal of budling safer autonomous vehicles. The lower the risk, the more efficient the method.

The second criterion shows the feasibility of the solution. Theoretically, many solutions could be implemented. However, feasibility plays a significant role in the matter as an easier implementation leads to more marketized methods that benefit the public. Hence, the more feasible it is, the better it becomes.

The third criterion shows how susceptible a solution is to fall to cyber-attacks. The more secure a solution is, the better. As seen in the last years, cybersecurity has played an immense role in the world's economy and in the public's safety. Therefore, it is an important point to address during the analysis of the proposed solutions.

III. Analysis

The following analysis is done based on the criteria above. It is ordered in a way to compare all solutions by one criterion and concluding the best solution based on it. Then, the result of each comparison is taken to finally prove why communication protocols are the best solution.

A. *Effectiveness*

Safety systems based on LiDAR and other sensors such as thermal sensors are efficient methods that provide vehicles with minute detection of their surroundings. As shown in in fig. 3, the more sensors the more precise the detection of obstacles, even in unfavorable conditions such as rain and night. By combining both a LiDAR and a thermal infrared camera, there appears to be low risks of accidents as the evidence shows. The probability of detection of objects varies between 85% to 100% depending on the environment, making the rate of accidents at most 15%.

Test Environment	**Obstacle Detection Probability**		
	LiDAR only	***Thermal Infrared Camera only***	***The Proposed (Combined)***
Night	0.45	0.75	0.85
Foggy (water spray)	0.8	0.75	0.9
Small Target (model of man)	0.85	0.9	1.0

Fig. 3 Comparison of obstacle detection probability [7]

High-precision maps also show great promise in the field of autonomous vehicles. A more precise mapping system allows vehicles to precisely calculate both their speed and position within a road. This information becomes crucial as when accidents occur as depending on where the potential danger is and how fast the vehicle is moving, the central computer of autonomous vehicles can decide accordingly. By implementing a more precise mapping system, more accurate numbers can be calculated and hence lower the rate of accidents as seen in fig. 4.

EV speed $[km/h]$	Impact speed at jaywalker incidents $[km/h]$					
	≤ 10	[10-20]	[20-30]	[30-40]	> 40	Avoidance
30	0.01%	0.001%	0.0001%	0.00001%	N.A.	~ 100%
40	0.1%	0.01%	0.001%	0.001%	N.A.	~ 99.9%
50	5%	0.1%	0.01%	0.001%	0.0001%	~ 94.9%
60	5%	5%	0.1%	0.01%	0.001%	~ 89.9%
70	10%	5%	5%	0.1%	0.01%	~ 79.9%
80	10%	10%	5%	5%	0.1%	~ 69.9%
90	10%	10%	10%	5%	5%	60%
100	10%	10%	10%	10%	10%	50%

Fig. 4 Impact speed probability with jaywalkers, given perception limitations (blue) and evasive ability limitations (white) [8]

As for communication protocols, the main efficiency issue that they face is related to interferences and jamming of the signals in medium and long-range communication such as V2V and V2I. Therefore, the lower the interferences possible, the higher the precision of communication. To improve the V2V and V2I communication, DJI Mavic 2 Pro, the same type of communicators used in communication between planes can be used, its operating frequency lies between 2.403 GHz and 2.465 GHz. When faced with jamming, it changes its exact frequency so that the jamming cannot interfere with it [9]. While not having an exact percentage for autonomous vehicles, it has proved very efficient in aerial transportation as the rate of plane accidents is relatively low.

Based on this criterion, we can see that communication protocols are more efficient than the other two solutions.

B. *Feasibility*

This second criterion comes with an easier analysis as it does not require as much experimentation as the previous one. It is based on "how easy" it is to carry through a solution.

Backup safety systems consist of a variety of sensors and captors that are already existing and used in other fields. Therefore, implementing such technology to autonomous vehicles only comes with minor changes. Adding new

sensors to the already existing autonomous cars does not come at a relatively high cost nor at high difficulty. This ease gives this solution much popularity within the industry and professionals.

For high-precision maps, the technology used is based on already existing systems such as GPS. However, it still is much more costly as it requires the upgrade of not only captors of the vehicles but may require the use of funds to work on already existing satellites that are used for mapping. This solution comes at a significant cost compared to the previous one.

As for communication protocols, they are based on already known technology but require a higher budget than the first solution but still lower than the second solution. Moreover, the ease of implementation is also moderate as this solution requires in-built communicators for short range communication, such as the inter-vehicle communication, medium-range communication, such as V2V communication. The difficulty comes from the V2I communication which is considered as long-range communication and requires more infrastructural communicators such as antennas.

Based on this criterion backup safety systems distinguish themselves as the better solution, followed by communication protocols, then high-precision maps.

C. Cybersecurity

Cybersecurity in autonomous vehicles is a critical factor for ensuring autonomous vehicles users' safety. By improving the defenses of the software of self-driving vehicles, the industry can flourish without the fear of cyber attacks that could harm both the users and their profit.

Safety systems such as LiDAR can easily fall prey to such attacks. Several studies proved that the carrier network of the vehicle and light detection radars are known to fall to these types of attacks which leads to a loss of control of the steering wheel and brakes and a misinformation of the central system of command [3]. As found in [10]:

> A bright light appeared on the vehicle's windshield; it would appear solid for 5-seconds every about 4 seconds. The designed bright light blocked the driver's forward view of the road and blinded the vehicle's sensors. After about 30-seconds of the flashing light, the vehicle would collide with a pedestrian, unless the participant stopped the vehicle during the attack. This scenario represented sensors being blinded through either extreme sun exposure or a nefarious bright light aimed to blind the vehicle sensors [10].

Similarly, sensor-coordinates that work to pinpoint the position and speed of a vehicle using GPS lack a sufficient level of cybersecurity which can lead to an alteration of routes followed by the vehicle [3], resulting in the danger of accidents or harm to the user.

As for communication protocols, they too are susceptible to these attacks. However, new research works on encrypting messages sent via V2V and V2I communications to lower risks of cyber attacks [11]. This makes communication protocols potentially safe from hacking and outside attacks.

Based on this third criterion, communication protocols prove to be safer in terms of cybersecurity compared to redundant safety systems and high-precision maps.

IV. Conclusion

Based on the given evidence and the analysis above, communication protocols prove to be the best solution among the three solutions proposed. They stand out as a highly efficient method with a relatively low cost and immune to most vicious outside cyber attacks.

However, this solution still has limitations related to cybersecurity. Experiments and tests may show that by encryption or other methods, communication protocols can become secure, but real-world applications may show the opposite. The field of technology is on an exponential growth and will always evolve. Therefore, the solution proposed must also be evolved accordingly to keep it viable.

References

[1] Y. Ma, S. Yang, J. Lu, X. Feng, Y. Yin and Y. Cao, "Analysis of autonomous vehicles accidents based on DMV reports," 2022 China Automation Congress (CAC), Xiamen, China, 2022, pp. 623-628.

[2] J3016: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles, 2021, [online].

[3] J. M. Qurashi, M. J. Ikram, K. Jambi, F. E. Eassa, and M. Khemakhem, "Autonomous vehicles: security challenges and game theory-based countermeasures," Jan. 2023.

[4] R. Huber, Kilian, A. Wetzel, E. B. Neitzel, and T. Brandmeier, "Light analysis for optimized object detection with cameras for integrated safety systems," Jul. 2022.

[5] L. Chen, F. Zheng, X. Gong, and X. Jiang, "GNSS high-precision augmentation for autonomous vehicles: requirements, solution, and technical challenges," vol. 15, no. 6, pp. 1623–1623, Mar. 2023.

[6] P. Koopman and M. Wagner, "Autonomous vehicle safety: an interdisciplinary challenge," IEEE intelligent transportation systems magazine, vol. 9, no. 1, pp. 90–96, 2017.

[7] M. Cho, "A study on the obstacle recognition for autonomous driving RC car using LiDAR and thermal infrared camera," Jul. 01, 2019.

[8] G. Rodrigues, R. Kianfar, and M. Brännström, "Precautionary safety for autonomous driving systems: adapting driving policies to satisfy quantitative risk norms," Sep. 2021.

[9] P. Kozak, V. Platenka, and M. Vrsecka, "Analysis of communication protocols of UAV control sets," Oct. 2022.

[10] S. Aliebrahimi and E.E. Miller, "Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles," May 2022

[11] M. Hussain and J.-E. Hong, "Enforcing safety in cooperative perception of autonomous driving systems through logistic chaos map-based end-to-end encryption," Dec. 2022.