International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 1
January 2019

Autonomous vehicles: challenges, opportunities, and future implications for transportation policies

Kanika Chourasia
Comp. Sc. & App. Dept., S.D. College (Lahore), Ambala Cantt, India
kanikab1002@gmail.com

ABSTRACT

Autonomous vehicles are future of Smart Cities. In this paper challenges faced by autonomous vehicles are discussed. What are the future implications for transportation policies we can opt? How artificial intelligence is helping in autonomous vehicles. With the advancement of technology autonomous vehicles can be used safely in future. What technology is being used today in autonomous vehicles? What can be used in future? This paper also discuss benefits of autonomous vehicles.

KEYWORDS

Autonomous vehicles, future vehicles, Autonomous cars, Smart Cities and smart vehicles, Driverless cars

1. How AI is driving the future of autonomous cars

Over the past decade, explosion of autonomous vehicle technology has seen in the United States that has swept across the auto industry. Major companies like Tesla, **Jaguar Land Rover,** BMW, Ford, **Samsung,** Audi, and even Google are working on autonomous vehicles technology. While many have only started hearing about autonomous technology recently.

An article in IEEE Spectrum in 1969 on autonomous vehicle technology is one of the earliest research publications. Lead engineers Robert E. Fenton and Karl W. Olson hypothesized that the future of automated vehicles would rely on "smart infrastructure" In that article. Smart infrastructure would guide the cars on roadways.

We have witnessed extraordinary advancement in computer technology and information systems in last few decades. Because of these advancements smaller and lighter computers have been developed. As a result, autonomous vehicles currently depend on locally available advancements and best in class PCs to watch and process their environment.

Computer's ability to understand their surrounding and to make decisions based on relevant information has also improved. Artificial Intelligence (AI) plays an essential role in the progress of self-driving vehicles.

2. AI: the brain of autonomous vehicles

Self-driving cars understand the world around them with the help of sensors. Sensors acts as a human brain that collects process and chooses specific actions based on information gathered.

Self-driving cars and each autonomous vehicle is equipped with advanced tools to gather information, including long-range radar, **Ultrasonic Sensors**, LIDAR, cameras, short/medium-range radar.

Each technologies collects different information. Each technology is used for special purpose. However, if this information is not processed and some form of action is not taken based on the gathered information then it is useless.

With the help of Artificial Intelligence autonomous vehicle can work like a human brain. Actual goal of Artificial Intelligence is for a self-driving car to conduct in-depth learning.

"Deep learning is the best enabling technology for self-driving cars". Sensors, cameras, radar and LIDAR are useful in deep learning. Brain is needed to make an autonomous car work safely and understand its environment and surroundings.

Some applications or obvious functions of Artificial Intelligence for these vehicles are:

- When vehicle is running low on fuel. It should direct itself to a gas station or recharge station.
- After knowing the current traffic conditions vehicle should adjust the trip's directions to find the quickest route.

- In order to communicate with passenger's speech recognition should be incorporated.
- Driver monitoring can be improved with Eye tracking.
- Natural language interfaces and virtual assistance technologies.

3. Helping autonomous cars learn from each other

Artificial Intelligence is a complex algorithm that imitates how the human brain learns. Instead of hard-coding an autonomous car with thousands of "If-Then" statements, software engineers create an algorithm to tell car's onboard computers what is right, wrong, safe, and unsafe for the car to perform.

Artificial intelligence algorithms are the only solution to the dynamic driving conditions on roads.

Engineers cannot hard-code every possible variable or situation a car may face in a daily drive. Instead, engineers rely on the ability of the autonomous car to collect information and then process it through the fluid Artificial Intelligence algorithm.

Autonomous cars have one advantage over human drivers that is self-driving cars have the ability to share their experiences and readings with other cars instantaneously.

Autonomous cars share Information and situations encountered by them along every mile driven with other vehicles so that each computer can take advantage of that information. Other vehicle can adapt itself to the environments faced by other vehicles.

This type of shared experience and active learning creates a situation where autonomous cars, through Artificial Intelligence algorithms, can enhance their capacity to respond to circumstances out and about without really encountering those situations first-hand.

4. The software for smarter cars tomorrow?

Unimaginable innovation in hardware, software, and computing capabilities helped in rapidly evolving of Self-driving cars. The factor which is restricting the growth of this field is Artificial Intelligence and machine learning.

Unless autonomous cars can interpret the many types of objects and situations surrounding them, autonomous vehicles can't make adequate decisions. Instead of developing millions of rules, all what we need is sophisticated learning algorithm which is needed to develop and standardized across the industry.

The future of autonomous cars depends on advanced Artificial Intelligence algorithms.

- BY 2020, 10 million autonomous vehicles will hit the roads.
- In 10 years completely independent vehicles will be the standard.
- Autonomous vehicles will generate a $7 trillion annual revenue stream by 2050.
- Widespread adoption of autonomous vehicles could lead to a 90% reduction in vehicle crashes.

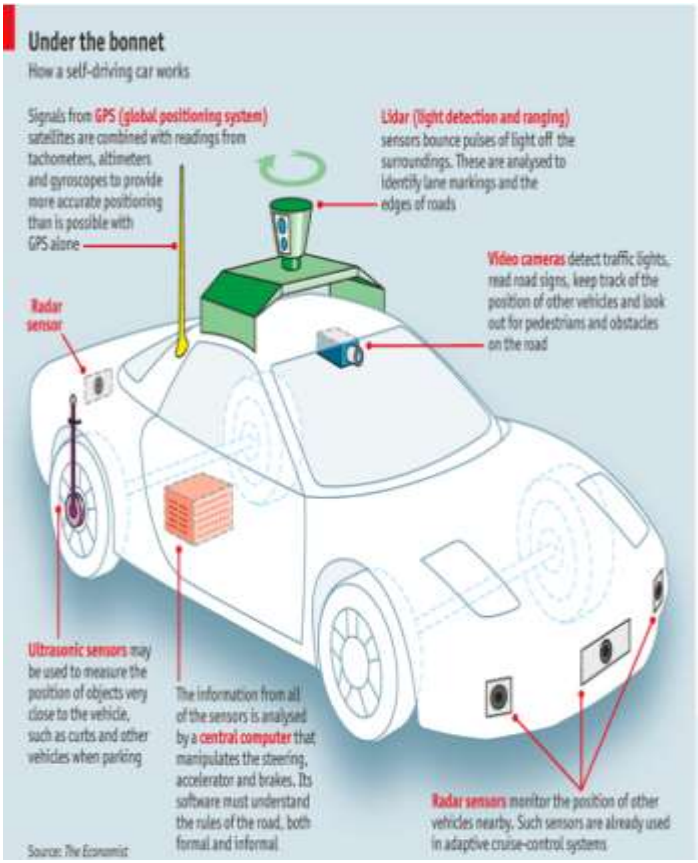
5. Key components of autonomous vehicles

- **Cameras** – Provide real-time obstacle detection. Which helps automated vehicles to facilitate lane departure and track roadway information (like road signs).
- **Radar** – Radio waves are used for detecting short & long-range depth.
- **LIDAR –** Light Detection and Ranging (LIDAR) Measures distance by illuminating target with pulsed laser light and measuring reflected pulses with sensors to create 3-D map of area.
- **GPS** – Global Positioning System Triangulates position of car using satellites. Current GPS technology is limited to a particular distance. Advanced GPS is in development.
- **Ultrasonic Sensors** – Uses high-frequency sound waves and bounce-back to calculate distance. Best in close range.
- **Central Computer** – "Brain" of the vehicle. The central computer receives information from various components which helps in directing the vehicle overall.
- **Dedicated Short-Range Communications-Based Receiver**– Permitting the vehicle to communicate with other vehicles (V2V) using DSRC. DSRC is a wireless communication standard. Which enables reliable data transmission in active safety applications.

6. Explanation of key attack gateways

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 1
January 2019

- **Electronic Control Units (ECUs)** – ECUs are embedded systems. ECU control one or more electrical systems or subsystems within a vehicle. ECUs are connected via an internal network. ECUs are used to control systems in the automated vehicle like steering and brakes, lighting, transmission and the engine, infotainment, etc. If access to ECUs (usually peripheral ECUs like an infotainment system) are breached and malicious actors are able to access certain ECUs or the whole network the risks arises. Vehicles today have up to 100 Electronic Control Units onboard.
- **On-Board Diagnostics (OBD) II Diagnostic Port**- Every car manufactured after 1996 and sold in the U.S. must have an OBD II installed. OBD II port was initially commanded to allow observing of emissions, etc. It is increasingly used to facilitate non-diagnostic features like enabling WiFi or enabling an insurance company to track usage through attachment of a "dongle" to the port. These ports can give methods for access to attackers into a generally secure system.
- **DSRC-Based Receivers** – DSRC is being advanced as a methods for urging V2V and vehicle-to-infrastructure (V2I) communications. The short-wave communications are more prone to spoofing and other attacks. There's presently a push to move to further developed 5G based communications.



7. Common security vulnerabilities

- **Software bugs** – Today automated vehicles contain more than 100 million lines of code. More lines of codes mean more opportunity for malfunction and mistakes. Glitches, even when inadvertent, can be exploited.
- **No Single Source of Knowledge or Control over Source Code** – Different developers are writing Software for different components of connected vehicles, and being installed by different supplies, and there are multiple sources so there is not a single entity that has knowledge of or control over the source code.
- **Increase Usage of Apps Leave Vulnerabilities** – Consumers are using an increasing number of smartphone apps to interface with their connected cars and help run certain functions. Researchers have already demonstrated weaknesses in some of these apps. Likely to see spread in use of malware.
- **Need for Constant Updates Maybe Overlooked** – With the increased use of connected

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 1
January 2019

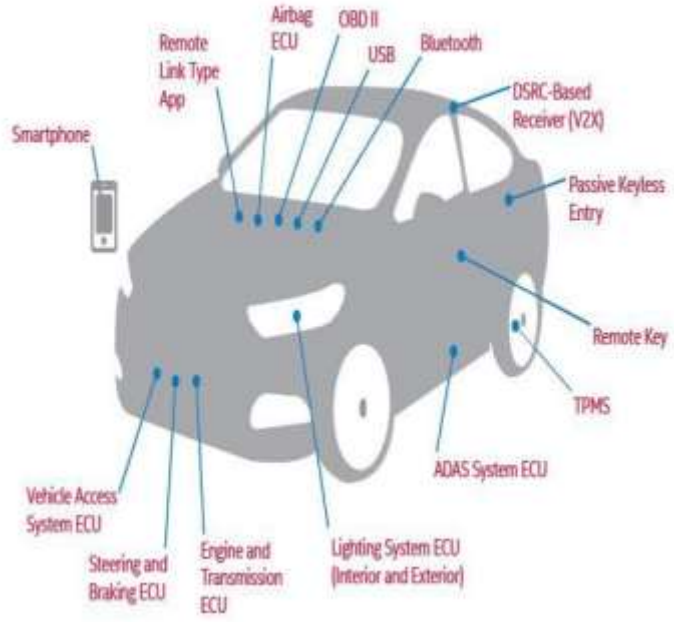
features comes an increased need for continuous updates to fix glitches and help protect vehicles. There is hazard these updates could be neglected or that malicious actors could taint routine updates.

8. Cybersecurity threats and concerns

- The same types of attacks that are possible in any connected device are generally possible in connected vehicles once access is gained.
- **For example** – Denial-of-service (DoS) attacks (e.g., utilizing the Controller Area Network (CAN) Bus system), remote access and control (The 2015 Jeep event), man-in-the-middle (MiM) attacks etc.
- The difference between attacks like these against common IoT devices and attacks within a connected or autonomous vehicle is the likelihood of increased risk to life and property in the vehicle context.

9. Litigation risks – cybersecurity

- Car manufacturers that release vehicles later found to contain defects and Cybersecurity vulnerabilities, along with the suppliers that provide flawed subparts, could face significant lawsuits in the U.S. and elsewhere.
- In 2015, after Chrysler recalled the Jeep Grand Cherokee to fix a flaw highlighted in the dramatic hack of the vehicle, the company and Harman International, maker of the defective Uconnect dashboard PC, confronted a high-stakes consumer lawsuit.
- In 2016, Dutch regulators sued Samsung over a lack of consistent updates to its Androidpowered phones. The controller battled that Samsung ought to be in charge of pushing refreshes two years after the clearance of a telephone. There is a plausibility comparative thinking could be connected to associated vehicle highlights.



10. Key cybersecurity takeaways

- **Provide Multi-layered protection** – Beginning at the level of individual ECUs, moving up a level to include software to protect vehicle's internal network by examining all network communications, and building in mechanisms to stop attacks from advancing within a network.
- **Defend against externally-facing potential gateways** – Ensure weakest links in car's security are viewed as potential threats and defenses are built into the system. This is especially consistent with infotainment or comparable remotely confronting systems that are created or used by different outside substances.
- **Ensure vendors and suppliers have strong security** – Connected and autonomous vehicles are made up of subparts and subsystems. It is critical to review and monitor vendor and supplier policies and practices.
- **Timely updates** – Companies should provide updates timely and effective fixes as soon as problems are identified.

11. Areas of innovation

- **Autonomous Driving: Autonomous Driving** is used to navigate a vehicle without human input from passengers. It uses sensor (LIDAR), control, and navigation equipment that responds to the environment when traveling.
- **Driver Assistance:** Safety and improved driving can be achieved when the driver is in control. Technology includes blind-spot detection, pedestrian detection, lane-departure warnings, intelligent braking, traffic-sign recognition, automatic braking, and adaptive cruise control.
- **Telematics: Telematics** Includes telecommunications, road safety, vehicular technologies, electrical engineering (sensors, instrumentation, wireless communications, etc.), road transportation, computer science (multimedia, Internet, etc.), GPS technology, DSRC, V2V, and V2I.

12. Key technology areas

- **Artificial Intelligence (AI)** –Automated vehicle can operate in a full range of environments with millions of changing aspects that will need to be accounted for, it will require AI, which will allow the base level software to be developed and tested with a self-learning capability.
- **GPS** – Global positioning systems helps in determining location of automated vehicles as they move.
- **Dedicated short-range communications (DSRC)** – The ability for vehicles to communicate with each other ("vehicle-to-vehicle" or "V2V") and infrastructure ("vehicle-to-infrastructure" or "V2I").
- **LIDAR** – Light Detection and Ranging (LIDAR) is a radar system that emits a laser in a pattern similar to rotating radar, only in more discrete and densely-spaced increments. The reflected laser light is used to provide the AV information on the distance for each discrete laser emission.

REFERENCES

https://www.mcca.com/wp-content/uploads/2018/04/Autonomous-Vehicles.pdf