International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 4, August 2021, pp. 3013~3021
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i4.pp3013-3021

Autonomous vehicles: A study of implementation and security

Firoz Khan[1], R. Lakshmana Kumar[2], Seifedine Kadry[3], Yunyoung Nam[4], Maytham N. Meqdad[5]
[1]Higher Colleges of Technology, United Arab Emirates
[2]Hindusthan College of Engineering and Technology, Coimbatore, India
[3]Faculty of Applied Computing and Technology, Noroff University College, Kristiansand, Norway
[4]Department of Computer Science and Engineering, Soonchunhyang University, South Korea
[5]Al-Mustaqbal University College, Hillah, Iraq

Article Info

Article history:

Received Aug 1, 2020
Revised Dec 21, 2020
Accepted Jan 13, 2021

Keywords:

Autonomous vehicles
Cooperative driving
LiDAR
Security
Ultrasonic sensors

ABSTRACT

Autonomous vehicles have been invented to increase the safety of transportation users. These vehicles can sense their environment and make decisions without any external aid to produce an optimal route to reach a destination. Even though the idea sounds futuristic and if implemented successfully, many current issues related to transportation will be solved, care needs to be taken before implementing the solution. This paper will look at the pros and cons of implementation of autonomous vehicles. The vehicles depend highly on the sensors present on the vehicles and any tampering or manipulation of the data generated and transmitted by these can have disastrous consequences, as human lives are at stake here. Various attacks against the different type of sensors on-board an autonomous vehicle are covered.

Corresponding Author:

Yunyoung Nam
Department of Computer Science and Engineering
Soonchunhyang University
Asan 31538, South Korea
Email: ynam@sch.ac.kr

1. INTRODUCTION

Over the years the automobile industry has been technologically improving and growing significantly. The developments in incorporating computer systems and computerization of mechanical and manual functions have improved the features of vehicles. More and more new cars are incorporating driver assisting features like adaptive cruise-control, lane departure warning systems and self-parking systems among other features [1, 2]. These features have reduced human dependency for the vehicles and given rise to vehicles that are partly autonomous in nature. Additional features with the help of sensors and on-board cameras have given rise to self-driving cars. Pushing this envelope further is the development of autonomous vehicles. These are a step further where the vehicles can navigate from a source to a destination by the use of various technologies, without any human intervention. These autonomous vehicles have the potential to significantly alter transportation and how humans travel in the future on the roads. The benefits of autonomous vehicles are significant, be it in use for transporting the elderly and disabled, or in the use in dangerous war zones where human life loss can be expected [3]. Other benefits can include reduction in traffic congestion, reduction in fuel consumption and optimal usage of the road infrastructure. These vehicles further aid in reducing traffic accidents which in turn provides cascading benefits like reduction in insurance costs, reducing loss of human life. Other benefits include reduction in carbon emissions and lesser air pollution. Autonomous vehicles have various technologies like radars, sensors, global positioning system (GPS) and on-board cameras that help it to detect the surroundings and navigate. The parts of an autonomous vehicle are highlighted in Figure 1. The data which is sensed using these technologies are fed into advanced

control systems present in these vehicles. These systems make relevant decisions regarding navigation and interpreting obstacles that may be present. Also interpreted are traffic signals and signage that help the vehicle to have a smooth movement from a source to a destination while accounting for the nearby vehicles on the road. Even though there are various benefits of using autonomous vehicles, there are also issues related to these vehicles. The costs of these vehicles will generally be higher than the comparable non-autonomous vehicles. This is due to the high amount of technology present in these vehicles [4]. The technology itself is not mature enough and still at its early stages, where developments are happening by the day. Other issues include accountability of accidents, security issues of technologies used, privacy issues related to consumer data, insurance regulation issues.

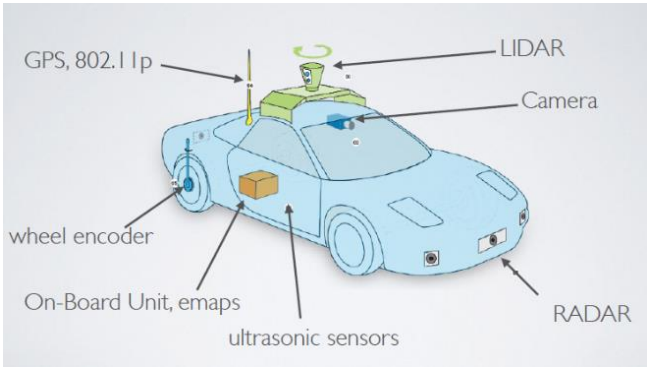

Figure 1. Autonomous vehicle components

Many companies including Google are involved in the development of these autonomous cars and several of the Google cars have competed around 2 million miles across various cities in the United States (US). But other companies like Uber technologies and Tesla motors are fast catching up and introducing their own autonomous vehicles on the roads [5]. This paper will be looking at the market penetration of autonomous vehicle and security issues related to the adoption of autonomous vehicle. Technological and non-technological issues related security of autonomous vehicles implementation will be looked at. The first section of the paper will address the benefits of autonomous vehicles, and the later part will cover the implementation issues with a specific look at security attacks against autonomous vehicles. The paper will be finished off by policy recommendations to address these issues with related to security and general adoptability of autonomous vehicles.

2. BENEFITS OF AUTONOMOUS VEHICLES

The automation system of automated vehicles follows three phases depicted in Figure 2 (i.e. `Sense', `Understand', `Act'). The automotive sector is going to be revolutionized by the adoption of autonomous vehicles. It needs to be seen if the adoption of these vehicles will outweigh and counteract the negatives associated with it. There are several benefits associated with the use of autonomous vehicles in transportations. The technology can be used in different type of vehicles like buses, where they can co-exist with a smart city to offer adaptive routes based on low and high-demand routes. They can also be used as taxis which can cater to people's needs. Another area of use is, heavy hauling trucks on long distance transportation between far reaching cities. These vehicles can also be effectively used in the military so that soldiers' lives are not put at risk while encountering dangerous warzones [6]. The following section will look at some of the far reaching benefits associated with autonomous vehicles and associated use [7].

2.1. Safety

These vehicles can be used to reduce the number of crashes on the road. It has been found that drivers are getting increasingly distracted behind the wheel with respect to drunk driving, speeding and increased usage of smartphones. This in effect is contributing to large losses in terms of currency, human lives and human injuries. The autonomous vehicles are programmed to avoid accidents and cause less disruptions in road traffic. However, having said that it was recently found that a driverless car from Uber went through a red light in San Francisco without stopping [8]. The autonomous vehicles are designed to navigate through any road infrastructure and has been successful to do so, so far. Advancements in

technologies used in these vehicles have made them much more dependable and safer even though the maturity of this technology has been challenging. Humans comprehending objects and traffic while driving is easier than autonomous vehicles and these have to be explicitly programmed and the evasive behavior depends on the object encountered by the vehicle. The vehicle has to successfully understand the situation at hand and come with a suitable counter-measure. If loss of human life is inevitable, then an important question to be asked is whether the safety of the vehicle occupants is more important than the safety of the pedestrians. These types of liabilities can be a huge hindrance for successful adoption. Another aspect of safety can be brought about by the creation of an ecosystem of cooperative vehicles on the roads [9]. For autonomous vehicles to be successful, an ecosystem consisting of road-side units (RSUs) and vehicle to vehicle (V2V) communication infrastructure needs to be developed. There needs to be a high level of interaction between these devices which will give rise to cooperative driving to increase the safety and functional benefits of autonomous vehicles.

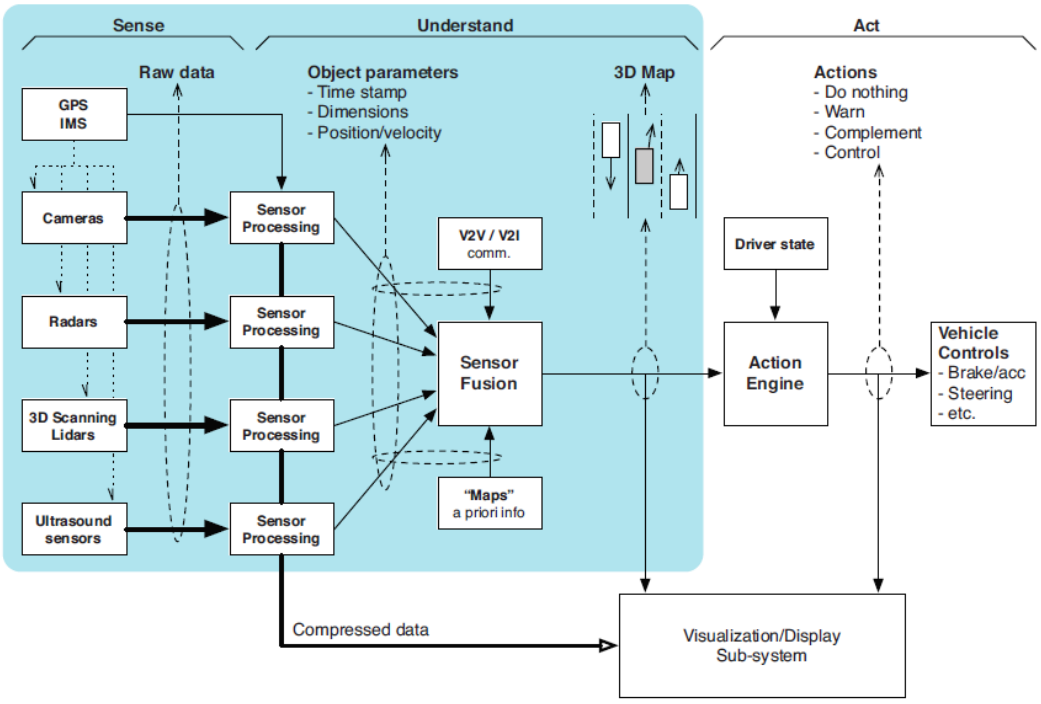

Figure 2. Data flow in an autonomous vehicle

2.2. Congestion and traffic management

The current state of road infrastructure is facing a huge amount of traffic congestion and tailback during peak times. These are primarily due to human's not anticipating slow upcoming traffic and normal stop and go durations. Another contributing factor is the low level of patience of drivers, where they change lanes frequently. The use of autonomous vehicles can help in coordinating traffic on highways and reduce tailbacks [9]. Autonomous vehicles can reduce the distances between themselves to have more vehicles on the road and the stop and go durations are considerably reduced. These in effect produces more efficient use of the roads infrastructure. Another benefit due to this, is the reduction in fuel consumption as the vehicle slowdown is reduced and thus carbon emissions are also reduced. Parking issues can also be considerably reduced in highly commercial areas. The autonomous cars can drop off their passengers where needed and go and self-park at a further parking area without human intervention. These vehicles can then be summoned to pick up its passengers when needed. These can give rise to parking savings on a large scale.

2.3. Human behavior

The autonomous cars can be a huge advantage for the people too young to drive, elderly and physically disabled [10]. These populations can be effectively transported from one location to another without any external person or aid. The cars can be used as mobile offices for working professionals and can provide entertainment while on a long distance commute. The benefit includes reduction of driver fatigue and

a smoother travel experience. A recent survey has found that more and more young people are opting to use public transportation rather than driving, as they would have more time to engage in other activities like browsing the internet or reading books. These people could be early adopters of autonomous vehicles. If there is an absence of public transportation in a city, shared autonomous vehicles can support the need of the residents of these cities. Humans depending on older technologies of mass transportation like trains can thus be reduced. Another potential benefit is avoiding the need to have private chauffeurs or the need to get driving licenses. Human error which can cause accidents, will be efficiently negated by the use of autonomous vehicles.

2.4. Adoption by specific sectors

The autonomous vehicle technology is being more and more adopted by various sectors like mining, freight transportation and the military among other industries. The trucking industry is adopting autonomous vehicle technologies to aid transportation over a large distance [11]. The adoption has reduced the need for drivers and increased fuel economy of these trucks. A behavior called as platooning is being used to by these trucking companies using a large number of autonomous vehicles which travel in tandem. In the mining industry, large autonomous earth movers are being used highly effectively. These earth movers have a fixed route from a source to a destination and are being very effective. The autonomous vehicles assist in improving the safety of humans as there are lesser number of people working around heavy equipment [12]. With autonomous mining vehicles, specialized equipment operators are not needed, which in turn improves productivity. The military sector is a huge embracer of autonomous vehicle technology. The military considers the autonomous vehicles as a huge enabler for its soldier protection [13]. Driverless military trucks can be deployed in sensitive areas to deliver essential items and commodities without human intervention.

3. IMPLEMENTATION ISSUES

Even though there are many advantages to implementing autonomous vehicles, its adaptability on a large scale is still in question. Studies on large scale implementations and its ramifications are still being done in real life environments and continuous further research is needed. The success of implementing autonomous vehicles depends highly on the costs associated with manufacturing, liability when accidents occur and licensing issues. Furthermore, as these are vehicles are operating using computing technologies, the security and privacy aspects is a very important field of study [14]. The following section will look some of the major inhibitors of adopting autonomous vehicles in a major scale.

3.1. Technology issues

The autonomous vehicles depend solely on its onboard sensors, GPS, light imaging detection and ranging (LiDAR) and camera systems. Any failure of these devices can contribute to serious consequences. Failures in sensors will need to be efficiently communicated and should be easy to detect and replace. Not just sensors, but computer and systems malfunctions can bring about disastrous consequences. These could be a major failure or even a minor glitch for essential items of an autonomous vehicles, like its braking system. All technologies on the autonomous vehicles have responded well during optimal conditions. But during extreme weather conditions, like hail storms, heavy rains or snowy conditions, the system will not operate perfectly and will interfere with the sensors and camera systems. Sufficient research on these areas still needs to be done to ascertain the reaction of these vehicles. Even if the autonomous vehicles can self-drive from a location to another, human intervention would still be needed to operate it safely. This could be an issue, as the future drivers could be heavily reliant on the technology and may have forgotten the necessary skills to successfully drive a vehicle. Pre-programming is done on the autonomous vehicles and the presence of artificial intelligence technologies help the vehicles to get accustomed to newer environments and situations on the road. A known limiting factor is that the vehicles are not programmed to interpret hand signals shown by other drivers or situations where the traffic is controlled by police officer manually using hand signals. Another issue is the reliability of dependency on GPS systems. Various examples have been found where people have been navigated to non-existent roads and bridges due to the inaccuracy of the technology.

3.2. Vehicle costs

A large scale adoption of autonomous vehicles will be seriously impeded due to the manufacturing costs of these vehicles. Various technologies including sensors, global positioning systems, communications from the vehicles and artificial intelligence software are needed for each vehicle. An essential piece of equipment, LiDAR, is very expensive currently and so are the processing requirement equipment. These prices put the autonomous vehicles cost beyond the purchasing power of average people who own cars. The success of autonomous vehicles can only be successful, if adopted on a large scale, which cascades on to

lower prices of the same vehicles in the future. This is like any technological adoptions, be it computers or electric cars, future prices can be reduced only with technological advances and large scale production. Even though early adopters may pay higher prices, the costs can be brought down in the future. This will remain a significant implementation challenge for the foreseeable future.

3.3. Liability and law issues

Even though autonomous cars have been tested for many thousand kilometers on public roads, still there are chances of accidents happening. This raises the concern of liability in case of such accidents. Who is at fault? Is it the person in the driver seat of the vehicle, the manufacturer or the algorithm developer? Another aspect is the insurance issues for such accidents [15]. In most cases humans are exempted from penalty when accident occur beyond the control of the driver. Legal precedents are also not existing in most countries where autonomous vehicles may be deployed. These are no existing laws or legalities around accidents involving autonomous cars. There are no central regulatory bodies existing country-wide to regulate the use of autonomous vehicles. Laws and rules applicable in one state may be different from another state.

3.4. Security and privacy issues

The most major issue with autonomous vehicles is in the field of security as there are numerous computing devices and communications occurring from the vehicle to other vehicles or various components within the vehicle itself. Hackers can get into the system and manipulate the operations of the vehicle [16]. This can be extremely dangerous as the vehicle can be controlled by people to do nefarious activities. Terrorist can use the vehicle loaded with bombs to target key establishments [17]. They can be also used as rolling missiles to target and create chaos on the roads. As vehicles are interconnected and communicate with each other, any malware can spread quickly through the entire vehicular network to penetrate a large number of vehicles. These malwares can be dangerous and can be used to do controlled and coordinated attacks. A security breach of autonomous vehicles will allow a hacker to do simple attacks like relaying false information from the sensors to taking complete control over all the operations of the vehicle. Security attacks against autonomous vehicles will be looked at in more detail in the next section. For the successful operation of an autonomous vehicle, lots of personal data is collected and stored. These data are shared among other vehicles and RSUs. The ecosystem of cooperative vehicles is built on the principle of sharing data [18]. This is a major concern for privacy advocates. Questions have been raised about what type of data will be stored, what will be shared, who will it be shared to, and what will the data be used for? Most humans do not want share the vehicular data as the data may be used against them in case of accidents and a court case. Also, the driving mannerisms will be used by insurance providers to increase the insurance costs if erratic driving behavior is observed. Location data is also tracked and shared by autonomous vehicles. This could enable tracking of users and can be misused by hackers for monitoring or even worse, can be used by criminals to track the location of victims.

3.5. Ethical issues

There are several non-technical ethical issues with the use of autonomous cars. Issues are being raised as to what to do in case of an emergency. Should the vehicle protect the occupants of the car or the pedestrians? Should the vehicle try to avoid animals crossing the street which may cause injuries to the passengers? How should the programming be done in such cases and who takes the decision during these programming? If the passenger is being robbed or being attacked by a criminal involving a carjacking, how should the autonomous vehicle respond? Can the vehicle run a red light or break traffic laws in an emergency? Other ethical issues faced would be how the vehicle to responds to rough, ignorant other non-autonomous drivers on the road. Should the vehicle take evasive measure when confronted with such situations? Ethical issues can be handled sufficiently by human drivers, but may not be handled in a humane way by the autonomous cars as, in the end, they are just machines running on programmed code. A high level of maturity is needed in the built-in processing software before the widespread implementation of autonomous vehicles.

3.6. Increased traffic

One of the major issue of convenience is the success and furthermore its overall usage. A major issue with the success of autonomous vehicles is its convenience. The more convenient it is, the more the number of people who will use it. This will give rise to increase in traffic due to unnecessary usage [19]. Earlier, with normal vehicles, when humans were feeling lazy for less critical travels, they would avoid the travel. But now, with autonomous vehicles, these may happen more often.

4. SECURITY ATTACKS

The manufacturers have been constantly working to improve the dependability of autonomous vehicles. These are primarily achieved by increasing the accuracy of data sensed by the various sensors on these vehicles. Tesla is considered to be a market leader in autonomous vehicles and even one of their cars, a Model S, crashed onto a truck and caused a death [20]. This accident highlights the importance of having accurate sensors that perform in normal road conditions. Even more important is the fact is that the sensors should not be vulnerable to external inputs and hacks. If external inputs or hacks are successful, then the sensors may produce false readings and sensor malfunctions [21]. This in effect will produce disastrous consequences on the road. The major categories of sensors used in autonomous vehicle are ultrasonic sensors, millimeter wave radars (MMW), on-board cameras, LiDAR and GPS [22]. Various attacks have been conducted against, both in- lab and in the external environment to test contactless attacks against these sensors. The attacks and its effects against each category of sensors will be reviewed in the following sections.

4.1. Attacks against ultrasonic sensors

The ultrasonic sensors are used to monitor the front and back of vehicle to detect obstacles and aid in the parking of a vehicle. The ultrasonic sensors work on the principle of emitting ultrasonic pulses and if an obstacle is present, these pulses are reflected back. The time taken to receive this reflected waves are measured, which is used to measure the distance of the obstacle from the sensor [23]. Following are some of the attacks conducted against ultrasonic sensors. Jamming attack-in a jamming attack an ultrasonic signal is created in the same frequency range as the vehicle's sensor operate and continually transmits the signal. Due to this the ultrasonic sensors does not detect obstacles and the vehicle collides with them. Spoofing attack-the same equipment used for jamming can be used to send ultrasonic signals, but instead of sending the signal continually, the spoofing signal is sent a specific time to trick the sensors. Due to this, the ultrasonic sensor detects an obstacle, even when one does not exist. Acoustic quieting method is used to hide the obstacles from being detected by an ultrasonic sensor. The sensors do not detect sound absorption materials like plastic foams and fur. If an object is covered with this material, the detection is avoided as the echoes as not returned by the material.

4.2. Attacks against MMW radars

MMW radars works using millimeter waves, which are considered to be waves whose frequencies are lesser than visible light but higher than the radio frequencies. These waves are transmitted out as probes and the reflections are measures to find various parameters including but not limited to examples like time and frequency difference. There are primary three types of MMW radars used on autonomous vehicles; Short range MMW radars used for blind spot detection, Medium range MMW radars used for collision avoidance and on road people detection, and long range MMW radars are used in adaptive cruise control systems at high speeds. A jamming attack against MMW radars are their effects are as seen below. Jamming attacks-a signal generator is used to send out constant signals in the same frequency range of the actual MMW radars on the vehicles. The jamming signals generated increases the noise levels and signal to noise ratio is considerably reduced. Due to this, the radar system existing on the vehicle fails and does not detect any vehicle or obstacle in front of it. This could lead to disastrous consequences where an autonomous vehicle may run into an obstacle in front of it.

4.3. Attacks against on-board cameras

On-board cameras use visible light and optics to comprehend visual recognition of the environment where the autonomous vehicle is being used. The cameras are especially useful in detection lanes, traffic signals and road signs. This data is used to enhance the driving and stopping capabilities of autonomous vehicles. The most major attack against on-board cameras is called as conducting a blinding attack. The goal of the attack is to affect the sensor of the camera by exposing it to a strong intensity light that temporarily blinds the camera from recognizing actual traffic signals or objects. Many type of light emitting devices can be used to conduct this attacks. Laser pointers and LED light sources are some of such prominent light emitting devices. It takes 4 to 5 seconds before the camera recovers from such a blinding attack. The attack can be done as a constant light source hitting the camera or exposing the camera to a burst of light. The latter is considered to be more effectively as the attacks cannot be easily detected and by the time the camera recovers, it is attacked again.

4.4. Attacks against the LiDAR system

LiDAR's are devices which use rotating laser beams. The device is used in the detection of obstacles and helps to navigate the autonomous vehicle through its surroundings. The data generated by the LiDAR system provides information about where obstacles exist in an environment and the position of the

autonomous vehicle with respect to the obstacle [24]. LiDAR data can show curvatures in roads, roadside infrastructure and vegetation and elevation of roads. Attacks on LiDAR system can create noise, fake reflections and spoof fake objects. Some attacks that can make this possible are highlighted below. Relay attack-the purpose of this attack is to relay the original reflected signal from an object to be coming from another position. This way the autonomous vehicle is tricked into understanding the false position of a real object as being either closer of farther away. The attack is conducted by using transceivers which receive the original reflected signal and retransmits it. This way the same reflected data is made to appear as coming and being detected in many locations. Spoofing attack-the previous attack can be extended further to generate non-existent objects and spoofed to trick the LiDAR system. The system detects several instances of the same object existing throughout its environment, which will hamper the optimal behavior of the autonomous vehicle.

4.5. Attacks against the GPS

GPS satellites are used by autonomous vehicles to identify geographic locations of themselves [25]. The geographic locations and vehicle identities provided by these satellites are a very important element for the success of autonomous vehicle implementation. Positioning attack-in this attack, a malicious user can exploit the behavior by using a GPS satellite simulator. This device can be used to provide false information about locations to unsuspecting vehicles, if the signal from this device is stronger than the authentic GPS satellites [26]. The vehicles are deceived to think they are in a different location than they actually are which will hamper the effective behavior of the autonomous vehicles. Also, another variant of the positioning attack is the tunnel attack, where GPS signals are temporarily not available in tunnels. An attacker provides false information about geographic positions once the vehicle leaves the tunnel and before it receives authentic GPS signals.

4.6. Attacks against the communication system

Denial of Service attacks is a very serious attack where the main aim is to prevent the authentic users from accessing the network and network resources [27]. The attackers transmit dummy messages into the network to overwhelm the current users, thus reducing the efficiency and performance of the network. This attack is very significant in nature such that, even if the attack is detected, it is very difficult to correct. In an ecosystem of cooperative vehicles, a vehicle can falsify a large number of fake identities and transmit dummy messages to other vehicles and RSUs [28]. These dummy messages can be misleading and can cause other vehicles to respond in unforeseen ways. Distributed denial of service (DDoS) attacks is a variant of the DoS attack where multiple vehicles collude and attack on a legitimate vehicle at one time from different locations. Multiple vehicles can attack a single vehicle from different locations and time, so that the target vehicle cannot communicate to other vehicles or the RSU. The wireless medium used in autonomous vehicle network, increases the possibilities of these attacks. Furthermore, the rapid change in topology and high mobility of vehicles aids in more instances of these attacks and detection becomes difficult.

5. RECOMMENDATIONS FOR SUCCESSFUL IMPLEMENTATION

Further detailed research needs to be done on autonomous vehicles and the technologies used in it. This will aid further expansion of autonomous vehicles and its penetration in the market. Guidelines needs to be created by government which aid the development and usage of autonomous vehicles. One such rule specified by the US Department of Transportation states that every vehicle on the roads of US should have V2V communications enabled by 2023 [29]. Successful V2V communication will enable autonomous vehicles to warn each other about traffic disturbances and obstacles [30]. Standards needs to be created for data storage and data communication which will aid development of unified standards [31]. These will in turn help manufacturers create autonomous vehicles without worrying about liabilities in case of failure.

6. CONCLUSION

Autonomous vehicles are not a distant future and vehicle manufacturers are embracing the technology where leading manufacturers are foraying into this field. These vehicles depend on on-board sensors and technical equipment for successful navigation and understanding the environment it is present in. Valid and accurate sensor data is critical for the successful router planning, emergency maneuvers and route calculations. In this paper, the major success factors and inhibitors of autonomous vehicles have been discussed. The paper also discusses a critical aspect of security of autonomous vehicles and why security is important. Security attacks on various sensors and on-board cameras have exposed several vulnerabilities of the autonomous vehicles. Also critical for autonomous vehicles success is the presence of wireless technologies for cooperative driving. The autonomous vehicles collect a variety of data from other vehicles

and their surroundings. The wireless connectivity exposes the vehicles to DoS and malware attacks. For efficient implementation, a secure wireless technology which encompasses the highest level of privacy and security is critical.

ACKNOWLEDGEMENTS

This work was supported by the Soonchunhyang University Research Fund.

REFERENCES

[1] Jafarnejad, S., Codeca, L., Bronzi, W., Frank, R. and Engel, T., "A Car Hacking Experiment: When Connectivity meets Vulnerability," *2015 IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, 2015, pp. 1-6.
[2] Coppola, R. and Morisio, M., "Connected Car: technologies, issues, future trends," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, 2016, Art. no. 46.
[3] "Driverless Cars- Robots Are Taking the Wheel," 2018. [Online]. Available: https://www.bloomberg.com/quicktake/driverless-cars.
[4] Driggs-Campbell, K. R., Shia, V. and Bajcsy, R., "Decisions for autonomous vehicles: integrating sensors, communication, and control," *Proceedings of the 3rd international conference on High confidence networked systems*, 2014, pp. 59-60.
[5] "Google's Self-Driving Car Project Is Losing Out to Rivals," 2016. [Online]. Available: https://www.bloomberg.com/news/articles/2016-09-12/google-car-project-loses-leaders-and-advantage-as-rivals-gain.
[6] "The Benefits and Challenges of Autonomous Vehicles," 2017. [Online]. Available: http://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/12838/The-Benefits-and-Challenges-of-Autonomous-Vehicles.aspx.
[7] Fagnant, D. J. and Kockelman, K., "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," *Transportation Research Part A: Policy and Practice*, vol. 77, pp. 167-181, 2015.
[8] "Driverless Uber Car Runs Red Light on First Day," 2016. [Online]. Available: http://www.huffingtonpost.ca/2016/12/15/driverless-uber-runs-red-light_n_13648684.html.
[9] "The Massive Economic Benefits of Self-Driving Cars," 2014. [Online]. Available: http://www.forbes.com/sites/modeledbehavior/2014/11/08/the-massive-economic-benefits-of-self-driving-cars/#2146f6e468d9.
[10] "The 3 biggest ways self-driving cars will improve our lives," 2016. [Online]. Available: http://www.businessinsider.com/advantages-of-driverless-cars-2016-6/#traffic-and-fuel-efficiency-will-greatly-improve-2.
[11] Gerdes, R. M., Winstead, C. and Heaslip, K., "CPS: an efficiency-motivated attack against autonomous vehicular transportation," *Proceedings of the 29th Annual Computer Security Applications Conference*, 2013, pp. 99-108.
[12] "Autonomous haulage: making mining safe and more productive today," [Online]. Available: http://www.cat.com/en_US/articles/customer-stories/mining/autonomous-haulage-making-mining-safer-and-more-productive-today.html.
[13] "Behind Tesla's Headlines, the Military Drives Autonomous Vehicles," 2016. [Online]. Available: http://www.forbes.com/sites/jeffmcmahon/2016/10/21/behind-teslas-headlines-the-military-drives-autonomous-vehicles/#6bae10304643.
[14] "Advantages and Disadvantages of Driverless Cars," 2020. [Online]. Available: https://axleaddict.com/safety/Advantages-and-Disadvantages-of-Driverless-Cars.
[15] "Self-Driving Vehicles Offer Potential Benefits, Policy Challenges for Lawmakers," 2014. [Online]. Available: http://www.rand.org/news/press/2014/01/06.html.
[16] "Hackers can trick self-driving cars into taking evasive action," 2015. [Online]. Available: https://www.theguardian.com/technology/2015/sep/07/hackers-trick-self-driving-cars-lidar-sensor.
[17] "Top 20 Pros and Cons Associated With Self-Driving Cars," [Online]. Available: http://www.autoinsurancecenter.com/top-20-pros-and-cons-associated-with-self-driving-cars.htm.
[18] Dominic, D., Chhawri, S., Eustice, R. M., Ma, D. and Weimerskirch, A., "Risk Assessment for Cooperative Automated Driving," *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 2016, pp. 47-58.
[19] Kouatli, I., "The non-technical issues with autonomous vehicles," *2015 International Conference on Connected Vehicles and Expo (ICCVE)*, 2015, pp. 52-53.
[20] "Tesla. A tragic loss," 2016. [Online]. Available: https://www.teslamotors.com/blog/tragic-loss.
[21] Xue, M. and Roy, S., "Characterization of security levels for the dynamics of autonomous vehicle networks," *2012 IEEE 51st IEEE Conference on Decision and Control (CDC)*, Maui, HI, USA, 2012, pp. 3916-3921.
[22] Petit, J., Stottelaar, B., Feiri, M. and Kargl, F., "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, no. 2015, 2015.
[23] Yan, C., Xu, W. and Liu, J., "Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle," *DEF CON*, vol. 24, no. 8, p. 109, 2016.
[24] "LIDAR Hacks Fairly Unlikely Attacks on Self-Driving Cars," 2015. [Online]. Available: http://www.roboticstrends.com/article/lidar_hacks_fairly_unlikely_attack_on_self_driving_cars.

[25] "Hacking Driverless Vehicles," [Online]. Available: https://www.defcon.org/images/defcon-21/dc-21-presentations/Zoz/DEFCON-21-Zoz-Hacking-Driverless-Vehicles.pdf.
[26] Gongjun Yan Yan, Gyanesh Choudhary, Michele C. Weigle, and Stephan Olariu. "Providing VANET security through active position detection," *Computer Commuication*, vol. 31, no 12, pp. 2883-2897, 2008.
[27] Alheeti, K. M. A. and McDonald-Maier, K., "Hybrid intrusion detection in connected self-driving vehicles," *2016 22nd International Conference on Automation and Computing (ICAC)*, Colchester, UK, 2016, pp. 456-461.
[28] Amoozadeh, M., Raghuramu, A., Chuah, C. N., Ghosal, D., Zhang, H. M., Rowe, J. and Levitt, K., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126-132, 2015.
[29] "The Feds Want All New Cars To Talk To Each Other By 2023," 2016. [Online]. Available: http://jalopnik.com/the-feds-want-all-new-cars-to-talk-to-each-other-by-202-1790059357.
[30] Reger, L., "Securely connected vehicles-what it takes to make self-driving cars a reality," *2016 21th IEEE European Test Symposium (ETS)*, Amsterdam, Netherlands, 2016, pp. 1-1.
[31] "Don't Believe The Hype About A Driverless Society Being Just A Few Years Away," 2016. [Online]. Available: http://jalopnik.com/dont-believe-the-hype-about-a-driverless-society-being-1790269631.