British Journal of Global Ecology and Sustainable Development
Volume- 44, September 2025
ISSN (E): 2754-9291

GUARDING THE FUTURE OF MOBILITY: CYBER THREATS AND DEFENSES IN AUTONOMOUS VEHICLES

Sherali Shirinov Ramazon o'g'li
TIIAME National Research University
shsherali92@mail.ru

Nurali Salimov Ramazon o'g'li
Northumbria University Newcastle MCs Cyber Security
nsalimov97@yahoo.com

Abstract
Autonomous vehicles (AVs) are transforming mobility with their integration of sensors, artificial intelligence, and interconnectivity. While these systems promise safety, efficiency, and sustainability, they also expose AVs to unprecedented cybersecurity risks. This article reviews major attack vectors—such as GPS spoofing, LiDAR manipulation, in-vehicle network intrusions, and wireless exploits—and highlights defensive strategies including biometric encryption, cryptographic protocols, and AI-based anomaly detection. Human awareness and regulatory oversight remain equally critical to strengthening resilience. The future of AV adoption hinges on layered cybersecurity approaches that safeguard passengers and public trust.

Keywords: Autonomous vehicles, cybersecurity, GPS spoofing, LiDAR jamming, biometric encryption, intrusion detection, regulation

Introduction

The rapid growth of autonomous vehicles marks a defining technological milestone of the 21st century. Using advanced perception tools such as cameras, LiDAR, radar, and GPS, AVs can navigate complex environments with minimal human intervention. These innovations promise to reduce traffic accidents, increase fuel efficiency, and improve accessibility. However, because AVs depend on digital infrastructure and constant connectivity, they are increasingly attractive targets for cyberattacks. Cybersecurity has therefore become a foundational requirement for ensuring both functionality and safety. Failures in AV cybersecurity could lead not only to financial loss but also to catastrophic accidents and disruption of public trust. Cybersecurity challenges in AVs thus extend beyond technical systems and into ethics, liability, and governance. This makes the issue not only a concern for engineers, but also for policymakers, regulators, and society at large.

Literature Insights

Research into AV cybersecurity demonstrates that threats emerge from both traditional IT vulnerabilities and physical-world manipulations. Koscher et al. experimentally demonstrated remote intrusions into modern vehicles, while Abdullah analysed how

Journal Zone Publishing, Ilford, United Kingdom

LiDAR can be deceived with basic equipment. Other studies show how camera-based perception systems are vulnerable to visual interference, and how GPS signals remain open to spoofing. The literature further notes that the growing reliance on Vehicle-to-Everything (V2X) communications increases the attack surface by introducing wireless channels.

Importantly, scholars distinguish between three primary categories of attack: perception attacks on sensors, communication attacks on wireless networks, and network attacks on in-vehicle communication systems. Together these categories provide a framework for understanding where defensive strategies must be applied.

Methodology

Approach: Mixed-methods combining literature analysis, threat modelling, and simulation/proof-of-concept experiments to evaluate attack vectors and defences for autonomous vehicles.

Data sources: Peer-reviewed papers, industry white papers, reported PoC attacks (GPS spoofing, LiDAR jamming, CAN injection), and vendor documentation.

Threat modelling: Systematic identification of attack surfaces (sensors, in-vehicle networks, V2X interfaces, supply chain). For each vector document entry point, attack mechanism, likelihood and impact.

Simulations / PoC: Reproduce representative attacks in simulation (e.g., ROS/Gazebo) or controlled lab setups where permitted; analyse sensor inconsistency and system degradation.

Defensive measures tested: Cryptographic authentication (PKI/OTA signing), hardware-backed keys, sensor-fusion consistency checks, and ML-based anomaly detection.

Evaluation metrics: Detection accuracy (precision/recall), false positive/negative rates, latency/compute overhead, and robustness under adversarial conditions.

Analysis methods: Quantitative evaluation of detectors and cryptographic overhead; qualitative synthesis of mitigation applicability and gaps from literature.

Ethics & safety: Use only authorized test environments; anonymize any personal data; follow legal and institutional review requirements.

Deliverable: Shortlist of prioritized attack vectors, assessed mitigations with measured trade-offs, and recommendations for deployment and future research.

Results, Analysis and Evaluation

There is a wide range of cyberattack types and procedures that may be used against autonomous vehicles. Some of these attacks make use of malicious software including worms, viruses, adware, and spyware. Others use social engineering techniques. Other kinds of attacks, in particular ones that aim to strengthen denial-of-service attacks, are carried out by certain attackers while others carry out man-in-the-middle attacks. The objective of cyber security is to forestall unauthorized access to autonomous vehicle

Journal Zone Publishing, Ilford, United Kingdom

(AV) systems through the use of personal computers, mobile devices, laptops, and other forms of wireless communication equipment.

This is primarily due to the fact that the operation of the vast majority of online browsers poses a risk to the functionality of these vehicles. This risk arises from the fact that browser-related cookies and programs can facilitate the transmission of malware and other potentially harmful entities. The global positioning systems (GPS) included in modern smartphones may be used to determine the location of other electronic devices. Cybercriminals have the ability to manipulate and exploit this information for malevolent purposes, such as tracking and snooping on the locations, plans, and activities of users, even if they do not have the users' consent. In the case of automobiles, cybercriminals can launch attacks on the GPS codes and systems in the vehicle, which not only wreak havoc on the vehicles' ability to function but also have the effect of leading both the drivers and the automobiles themselves to incorrect places.

It is quite clear that the communications component of everything is essential to the successful operation of these vehicles. As a result, it is of the utmost importance to devise methods and procedures that will ensure the connection and sharing of data between cars in a secure manner. This research suggests the use of biometric systems and data for identification and access control as a means of enhancing the security of communications in the context of managing the secure transmission of data and information between these automobiles. The research was carried out as part of an effort to determine how to manage the secure transmission of data and information between these automobiles.

A new authentication system should be implemented to replace the older setups, which rely on passwords for their protection systems and foundation, in order to achieve the goal of achieving simplicity in authentication and achieving a secure communication system for AVs. This will allow for the achievement of both of these goals. The prevention of unauthorized individuals and organizations from gaining access to sensitive and confidential information is the primary objective and purpose of applying message authentication techniques and systems to a specific set of messages or communications. Message authentication techniques and systems can be broken down into three main categories: In addition to being able to fulfil these security requirements, the use of biometrics provides a number of other benefits and advantages, such as simple access to services and a high rate of operational speed.

Human activities and other bodily features are analysed and used by biometric recognition systems to create a person's unique traits. It is thought that the iris of a human being is employed in the vehicle-to-vehicle identification processes in the innovative method that was provided in the work that was done on this study.

An autonomous vehicle, often known as an autonomous vehicle (AV), is a vehicle that has the capacity to drive itself and make its own decisions about how and where to go. Vehicles that can only be modified to a limited extent offer better handling and lower overall ownership costs. It is projected that fully automated cars would have direct control over all responsibilities, will not require a driver who is regularly available while

Journal Zone Publishing, Ilford, United Kingdom

the vehicle is in motion, and will not even require a steering wheel. Even automobile manufacturers have made the decision to prioritize driverless cars. It contributes to the development of passenger safety as well as the effectiveness of transportation by utilizing V2X and V2V linkages with the outside world (Kumar et al., 2018).

They do this by sharing data with one another, which may include the automobile's speed, position, and heading angle (Kroger, 2021). This helps them forecast where the car will be in the future. Utilizing information that has already been discovered, sensor technology makes it simpler to navigate both roads and fields. This is made possible by the data that has already been established. This kind of self-driving automation gathers environmental data without directly engaging with any other cars or infrastructures.

When it comes to vehicles of the future, there are a lot of benefits, such as the elimination of the requirement for extra-terrestrials to be able to respond rapidly, as well as the eradication of boredom and fainting while driving. The invention of the vehicle provided a solution to these issues. It also results in significant economic savings, including fewer social casualties and improvements to the environment. Additional fuel-efficient cars that are able to lower the amount of fuel they consume based on variables and sensors of this kind would also have a future in this scenario.

Research on autonomous driving systems for automobiles is expected to make strides in the not-too-distant future, which will lead to an increase in the prevalence of autonomous cars on public roadways. Analysts in this sector predict that self-driving autos will be within reach of the average consumer over the next five to ten years. As the rate of automation in the transportation sector continues to rise, so does the amount of press coverage given to self-driving cars. It has been proved how asymmetric algorithms can have an effect on extremely large amounts of data that are encrypted using a public key. The most significant barrier that must be overcome for autonomous vehicles is cyber security. The most important contribution that this study will make is to ensure that asymmetric algorithm technology will be used whenever data is kept in cloud storage. Since the first investigation, we have decided on and begun implementing two different strategies in the automotive industry. As a result of the method described in the thesis, there is the potential for two different hazard modelling methodologies to be utilized more frequently and deployed in a variety of vehicle systems. I have high hopes that the information obtained from this study, together with the outcomes of the threat modelling technique, will contribute to an improvement in the level of cybersecurity provided by connected vehicles.

The Vehicle-to-Vehicle, or V2V, technology permits wireless communication between vehicles and the maintenance of temporary networks to reduce the number of accidents and other issues associated with traffic (Ghosal and Conti, 2020). This information may refer to the protection and safety of the roadway, the maintenance of a safe distance between cars in order to avoid collisions, or any other information that is important to the vehicle. Due to the scattered nature of this technology, it is demanding, and automobile manufacturers will need to make compromises regarding the communication technologies that will be used to execute vehicle-to-vehicle contact.

Journal Zone Publishing, Ilford, United Kingdom

Only automobiles produced by the same manufacturer and with the same name will be authorized unless the respective manufacturers come to an agreement.

The concept of driverless automobiles is currently gaining traction in both the commercial world and the public conversation. Over the course of the last several decades, there has been a steady growth in the media's interest in self-driving vehicles, notably cars. Not only are there an increasing number of news sources aimed at businesses that create technology for driverless vehicles, but there are also an increasing number of news sources aimed at customer experiences with driverless vehicles. Recent news pieces, for example, have focused on self-driving automobiles, including improvements in self-drive technology, advantages for aged and disabled vehicles, and, of course, tragic ones self-driving autos murdering a pedestrian. The concept of driverless cars comes up repeatedly whenever important advances are made in technology, society, or politics. Despite the fact that not all of this improvement is favourable. Driverless technology (like as autonomous braking systems and lane-shifting assistance, for example) may also make it possible for businesses to run certain levels of responsible goods in a way that is both safe and effective. Automatic notifications are sent out to consumers, manufacturers, and developers if there is a problem with the dependability or safety of autonomous driving systems.

The impact of the media on consumers' expectations regarding self-driving automobiles may be largely blamed for this development. It is possible that the titles of news articles are slightly prejudiced, which can either help or hinder the general public's image of certain autos and, as a result, play an important role in modifying the expectations and actions of customers.

Automobiles capable of driving themselves, often known as autonomous vehicles or self-driving cars, are the most game-changing technical development of the last century. A automobile that is fully autonomous has the ability to recognize its surroundings, select the most direct route, and drive itself without assistance for the entirety of the trip. The concept of driverless automobiles has the potential to significantly reduce the number of accidents, the amount of time spent traveling, and the negative effects on the environment. However, there are still obstacles in the way of the widespread implementation of the technology, such as the requirement to allay public apprehension, enhance its usability, and govern it in an appropriate manner.

Computing in the cloud has emerged as an appealing resource for the day-to-day operations of end users. This is the case for a variety of reasons, the most important of which are its exceptional scalability, extensive capabilities, and on-demand access to a shared pool of computing resources. It has become vital in fields including as web development, analytics for big data, and the Internet of Things because of its accessibility and its ability to quickly link across interconnected networks.

Discussion and Conclusion

The threats reviewed demonstrate that no single solution can secure autonomous vehicles. Instead, a layered defence combining secure hardware, robust encryption, AI-

Journal Zone Publishing, Ilford, United Kingdom

driven monitoring, and human-cantered oversight offers the strongest approach. Furthermore, cross-industry collaboration is essential, as weaknesses in one manufacturer's systems can affect the broader transportation ecosystem.

The societal implications of insecure AVs are significant. Beyond accidents and disruptions, large-scale attacks could shake public trust, slow adoption, and reduce the benefits of automation. Conversely, strong cybersecurity foundations can accelerate adoption by ensuring that the public, regulators, and industry stakeholders have confidence in the technology.

Autonomous vehicles represent a major leap forward in mobility, but their dependence on interconnected systems exposes them to complex cybersecurity challenges. Attacks on GPS, LiDAR, cameras, CAN bus networks, and wireless communications illustrate the breadth of vulnerabilities. Defences must therefore be layered, integrating biometrics, cryptography, anomaly detection, and regulatory frameworks. Addressing these challenges proactively will ensure that AVs deliver on their promise of safer, smarter, and more efficient transport.

References

1. Abdullah, Q. (2016). A Star is Born: The State of New Lidar Technologies. Photogrammetric Engineering & Remote Sensing, 82(5), 307–312.
2. Ghosal, A., & Conti, M. (2020). Security issues and challenges in V2X: A survey. Computer Networks, 169, 107093.
3. Jan, S., & Tao, A. (2016). Comprehensive Comparisons of Satellite Data, Signals, and Measurements between the BeiDou Navigation Satellite System and the Global Positioning System. Sensors, 16(5), 689.
4. Koscher, K., Czeskis, A., Roesner, F., Patel, S., et al. (2010). Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy, 447–462.
5. Kumar, S., Tyagi, B., Kumar, V., & Chohan, S. (2020). Optimization of Phasor Measurement Units Placement Under Contingency Using Reliability of Network Components. IEEE Transactions on Instrumentation and Measurement, 69(12), 9893–9906.
6. Li, Y., & Ibanez-Guzman, J. (2020). Lidar for Autonomous Driving: Principles, Challenges, and Trends. IEEE Signal Processing Magazine, 37(4), 50–61.
7. Raiyn, J. (2018). Data and Cyber Security in Autonomous Vehicle Networks. Transport and Telecommunication, 19(4), 325–334.
8. Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. Future Internet, 11(4), 89.
9. Taeihagh, A., & Lim, H. (2018). Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, and Cybersecurity. Transport Reviews, 39(1), 103–128.

Journal Zone Publishing, Ilford, United Kingdom