IJARETY

International Journal of Advanced Research in Education and TechnologY *(IJARETY)*

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017

Mitigating Cyberattacks and Traffic Impact Analysis on Connected Automated Vehicles for Improved Safety

Sakshi Sharma[1], Natasha Dutta[2]

IT Project Manager, Promedia Telecom Inc., San Diego, CA. [1]

Security Analyst, Senior Executive, Vodafone Intelligent Solutions, Pune, India[2]

ABSTRACT: This study investigates the impact of cyberattacks on the dynamics of mixed Connected Automated Vehicle (CAV) traffic flow, focusing on scenarios where falsified velocity information is transmitted between vehicles. Using numerical simulations, we examine how overestimated and underestimated velocity messages affect traffic stability, safety, and road efficiency. The findings reveal that cyberattacks can lead to dangerous situations, such as reduced following distances and inefficient use of road capacity. However, the implementation of a Resilient Remote-Control Strategy (RRCS) effectively mitigates these adverse effects, maintaining stable and safe traffic flow even under attack. The study underscores the importance of robust cybersecurity measures, like RRCS, in future CAV systems to ensure both operational safety and efficiency. These insights contribute to the ongoing development of resilient and secure CAV technologies, which are essential for the future of automated transportation networks.

KEYWORDS: connected and automated vehicles, cyberattacks, mixed traffic, car-following model, resilient and robust control strategy, Artificial Intelligence (AI) in Vehicles, Fuel Efficiency, GPS Spoofing.

I. INTRODUCTION

The advent of Connected Automated Vehicles (CAVs) represents a transformative shift in the transportation industry, with the potential to significantly enhance road safety, reduce traffic congestion, and improve fuel efficiency. CAVs integrate advanced technologies such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, sophisticated sensors, and artificial intelligence (AI) to navigate roads autonomously while interacting with other vehicles and traffic systems. These interconnected systems allow CAVs to make real-time decisions based on a vast array of data, leading to smoother traffic flow, fewer accidents, and a more efficient use of road networks. However, the increasing connectivity and automation of vehicles also introduce new vulnerabilities to cyberattacks. As CAVs rely heavily on communication networks and onboard systems to operate safely and efficiently, they become prime targets for malicious actors seeking to disrupt transportation systems, compromise vehicle safety, or exploit personal data.

At present, the global innovation trend is surging, and a new round of industrial transformation is poised to take place. Internet, mobile communication, big data, artificial intelligence, and other new technologies accelerate breakthroughs and continue to evolve, promoting the rapid development of mobile Internet and automated driving technology. Connected and automated vehicles which can realize “safe, efficient, comfortable and energy-saving” driving will also emerge as the times require. CAVs are expected to improve the characteristics of traditional traffic flow from the micro vehicle level, and then provide an effective way to solve the problems of traffic congestion, traffic efficiency, and traffic pollution. Scholars have also carried out some research to demonstrate the great potential benefits of CAVs [1–3]. However, with the help of diverse and advanced communication technology, the “intelligent” information exchange between vehicles and the surrounding environment/world is realized all the time. Therefore, such an open-access communication environment system increases the risk of vehicles being exposed to cyberattacks, which is an urgent and critical challenge to be solved [4].

The cybersecurity challenges posed by CAVs are multi-faceted and complex. Cyberattacks on CAVs can manifest in various forms, ranging from direct attacks on vehicle control systems, such as hijacking a vehicle’s steering or braking functions, to more insidious methods like spoofing GPS signals, jamming communication channels, or spreading malware through vehicular networks. These attacks can have catastrophic consequences, including traffic accidents, loss of life, and significant disruptions to public transportation and logistics networks. Moreover, the interconnectivity of CAVs means that a breach in one vehicle’s system could potentially propagate to others, leading to large-scale traffic disruptions and a cascading failure of transportation infrastructure. As such, ensuring the cybersecurity of CAVs is not

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017

merely a technical challenge but a critical safety issue that requires comprehensive strategies for risk mitigation and impact analysis.

In terms of efforts to reveal the impact of cyberattacks on traffic flow characteristics, Amir et al. [5] investigated the influence of mobile reactive jamming attacks on the stability of CACC platoon, and the results showed that this attack will reduce the stability of traffic flow system. Wang et al. [6] proposed an extended car-following model to describe connected traffic dynamics under cyberattacks, the results showed that the proposed model will help to avoid collision and reduce traffic congestion under the influence of cyberattacks. Li et al. [7] studied and evaluated the impact of slight cyberattacks on CAV longitudinal security through modeling and simulation. The results showed that the impact of communication location attacks is worse than that of speed attacks. In addition, the impact of cyberattacks in vehicle acceleration phase is more severe and dangerous than that in vehicle deceleration phase. Wang et al. [8] proposed a bi-bi-layer architecture composed of both a vehicle layer and a cyber layer to explore the impact of cyberattacks on CAV platoon safety and efficiency. Dong et al. [9] proposed an evaluation framework to measure the impact of cyberattacks on traffic flow performance and analyzed and studied the impact from the aspects of attack intensity, attack range, and traffic demand through numerical simulation. Khattak et al. [10] used an infrastructure-based communication platform to discuss the impact of cyberattacks on the safety and stability of connected and automated vehicle platoons under lane changes.

Addressing these cybersecurity threats necessitates a holistic approach that combines robust security measures with a deep understanding of the potential traffic impacts of cyberattacks. Mitigating the risks associated with CAV cyberattacks involves implementing multiple layers of defense, including encryption, authentication protocols, anomaly detection systems, and fail-safe mechanisms that can prevent or minimize the damage caused by an attack. However, it is equally important to analyze how such attacks might affect traffic patterns and safety on a broader scale. For instance, a cyberattack that causes a sudden stop or erratic behavior in a single CAV could trigger a chain reaction of collisions or traffic jams, particularly in densely populated urban areas. By conducting detailed traffic impact analyses, researchers and engineers can better understand these dynamics and develop strategies to enhance the resilience of CAV systems to cyber threats.

Furthermore, in terms of countering the adverse impact of cyberattacks on traffic flow, Zhai et al. [11] designed a new continuous feedback controller based on lattice hydrodynamic model to suppress the impact of cyberattacks, and the effectiveness of the controller in dealing with cyberattacks and reducing traffic congestion were analyzed and verified by stability analysis and numerical simulation. Noei et al. [12] proposed a traffic microsimulation tool that can simulate conventional, automated, and connected and automated vehicles in a platoon under fault, failure, and cyberattack with optimized accuracy and simulation speed to maximize throughput and without compromising safety or string stability. Lyu et al. [13] designed a communication topology safety response system (CTSRS), and further combined with the distributed model predictive control (DMPC) to ensure the stability and security of the truck platoon even if the trucks suffer cyberattacks. Cheng et al. [14] proposes a novel intelligent driving model considering cyberattacks and heterogeneous vehicles and revealed that the traffic stability and safety under cyber-attacks can be enhanced through the high proportion of cars and the information accepted from cooperative vehicles ahead. In addition, some effective and robust control strategies that are not targeted at CAVs also need to be further studied and are worthy of being applied to deal with CAV cyberattacks [15,16], but we will not make a further detailed summary here.

Improving the safety of CAVs in the face of cyber threats requires collaboration across various stakeholders, including vehicle manufacturers, cybersecurity experts, transportation authorities, and policymakers. This collaboration is essential for developing standardized security protocols, sharing threat intelligence, and creating regulatory frameworks that ensure the safe deployment of CAVs. As the adoption of CAVs continues to grow, so too does the need for rigorous testing and validation of both the vehicles and the communication networks on which they depend. Only through such comprehensive efforts can the full potential of CAVs be realized, ensuring that the benefits of connected and automated transportation are not overshadowed by the risks of cyberattacks. Ultimately, the goal is to create a resilient and secure transportation ecosystem where the safety and efficiency of CAVs can be fully leveraged for the benefit of society.

II. REVIEW OF LITERATURE

The body of literature on Connected Automated Vehicles (CAVs) has expanded significantly in recent years, reflecting the growing interest in the potential benefits and challenges associated with these technologies. A central theme within this body of work is the dual focus on enhancing the operational capabilities of CAVs while simultaneously addressing the emerging cybersecurity threats that accompany increased connectivity. Researchers have explored a wide array of

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017

topics, including the technical architecture of CAVs, communication protocols, cybersecurity vulnerabilities, and the broader implications of these technologies on traffic safety and infrastructure.

One critical area of research has been the development of communication protocols that enable reliable and secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) interactions. Studies have highlighted the importance of robust communication standards, such as Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X), which facilitate real-time data exchange between vehicles and traffic management systems. These protocols are essential for ensuring that CAVs can operate safely in dynamic traffic environments, where timely and accurate information is crucial for making decisions such as lane changes, speed adjustments, and collision avoidance. However, the literature also underscores the challenges associated with securing these communication channels from potential cyber threats. For instance, researchers have identified vulnerabilities in the DSRC and C-V2X protocols, such as the potential for signal jamming, data spoofing, and unauthorized access, which could be exploited by malicious actors to disrupt vehicle operations or compromise driver safety.

Sliding Mode Control (SMC) is popular in control systems because it is robust, accurate, and relatively straightforward to implement. However, it comes with a challenge: the control gains need to be high enough to handle parametric uncertainties but low enough to avoid excessive chattering—a rapid oscillation that can degrade performance. Fine-tuning these gains is essential for balancing robustness with smooth operation. [16] This paper introduces a new method that enhances traditional sliding mode control by incorporating fuzzy logic to optimize its performance. The approach involves designing a fuzzy system that generates the right coefficients for the sliding mode controller. This optimization aims to achieve the best performance with minimal control effort, avoiding the need for complex expert systems and ensuring that the control outputs remain within the limits of the actuators.

Another significant focus of the literature is on the cybersecurity challenges specific to CAVs. The increasing complexity of CAV systems, which integrate multiple sensors, onboard computers, and external communication networks, has introduced numerous potential attack vectors. Scholars have explored various types of cyberattacks that could target CAVs, including attacks on the vehicle's control systems, such as braking and steering, as well as attacks on communication networks that could disrupt the flow of information between vehicles. [17] The literature has documented real-world incidents and experimental demonstrations of such attacks, providing concrete evidence of the risks involved. For example, studies have shown that a coordinated cyberattack on a fleet of CAVs could lead to widespread traffic disruptions, accidents, and even loss of life. As a result, there is a growing consensus among researchers that cybersecurity must be a top priority in the design and deployment of CAV technologies.

In response to these challenges, the literature has proposed various strategies for mitigating the risks associated with cyberattacks on CAVs. One common approach is the implementation of advanced encryption and authentication protocols to protect the integrity and confidentiality of data exchanged between vehicles and infrastructure. Additionally, researchers have emphasized the importance of developing intrusion detection systems (IDS) that can monitor CAV networks for signs of abnormal behavior or unauthorized access. These systems can serve as an early warning mechanism, allowing for timely intervention before an attack causes significant harm. The literature also suggests that fail-safe mechanisms should be integrated into CAV systems, enabling vehicles to enter a safe mode in the event of a detected cyber threat, thereby minimizing the risk of accidents or other adverse outcomes.

Beyond the technical aspects of cybersecurity, the literature also addresses the broader implications of CAV cyberattacks on traffic safety and infrastructure. Several studies have employed simulation models to analyze the potential traffic impacts of various types of cyberattacks on CAVs. These models allow researchers to assess how attacks might propagate through a network of connected vehicles, leading to traffic congestion, accidents, or even large-scale disruptions of transportation systems [18]. The findings from these studies have highlighted the importance of resilient traffic management systems that can adapt to disruptions and mitigate the impact of cyberattacks on road networks. Moreover, the literature points to the need for a comprehensive regulatory framework that sets standards for CAV cybersecurity and ensures that manufacturers and operators adhere to best practices for safeguarding against cyber threats.

The literature emphasizes the need for interdisciplinary collaboration in addressing the cybersecurity challenges associated with CAVs. Given the complexity of these systems and the potential consequences of cyberattacks, it is clear that no single discipline can tackle these issues in isolation. Instead, researchers argue for a collaborative approach that brings together experts in automotive engineering, cybersecurity, traffic management, and public policy. Such collaboration is crucial for developing holistic solutions that not only enhance the security of CAVs but also ensure that these technologies can be safely integrated into existing transportation systems. As the literature continues to evolve, it

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017

is likely that new insights and strategies will emerge, further advancing our understanding of how to protect CAVs from cyber threats and ensure their safe operation on the roads.

III. OBJECTIVE OF THE STUDY

The objective of the study is to:

1. Assess the impact of cyberattacks on mixed CAV traffic flow dynamics.
2. Investigate the effects of overestimated and underestimated velocity messages on vehicle safety and traffic efficiency.
3. Evaluate the effectiveness of the Resilient Remote-Control Strategy (RRCS) in mitigating the adverse effects of cyberattacks.

IV. METHODOLOGY

This study aims to assess the impact of cyberattacks on the dynamics of connected automated vehicles (CAVs) within a mixed traffic flow, focusing specifically on longitudinal car-following behavior. To achieve this, the research employs a simulation-based approach that integrates assumptions about vehicle behavior, cyberattack scenarios, and vehicle classification into a cohesive analytical framework. The methodology is structured around the simulation of CAV behavior under various cyberattack scenarios, the evaluation of traffic flow dynamics, and the comparison of these outcomes across different vehicle types.

4.1 Simulation Model Development

The first step in the methodology involves developing a simulation model that accurately represents a mixed CAV traffic flow. The model is based on the following assumptions:

Vehicle Types: The traffic flow consists solely of different types of connected and automated vehicles (CAVs). Non-connected or manually driven vehicles are excluded from the simulation to focus on the dynamics specific to CAVs.

Behavioral Focus: The study considers only longitudinal car-following behavior, meaning that lane-changing and overtaking maneuvers are not included in the model. This simplification allows for a more focused analysis of how cyberattacks influence vehicle dynamics along a single lane.

Cyberattack Exposure: It is assumed that cyberattacks can potentially target any vehicle within the CAV platoon. These attacks could disrupt the normal operation of the vehicles, thereby affecting traffic flow.

Limited Sensory Input: Each vehicle in the simulation only has access to its own position and velocity data. Vehicles receive information from the preceding vehicle via a communication device, which acts as a remote sensor. No additional sensors, such as radar, cameras, or LiDAR, are included in the model. This setup highlights the critical role of communication in maintaining safe and efficient traffic flow in CAV systems.

Neglected Delays: The model assumes that there are no delays in controller switching, actuator execution, or information transmission. This assumption simplifies the simulation and focuses on the immediate effects of cyberattacks on vehicle dynamics.

A schematic diagram (Figure 1) illustrates the CAV mixed traffic flow, capturing the various vehicle types and communication interactions among them.

4.2 Cyberattack Scenarios

The study explores different types of cyberattacks that could affect the dynamics of CAVs, particularly in terms of vehicle position, velocity, and acceleration. These attack scenarios are adapted from Wang's classification and are summarized as follows:

Position Attacks: These involve manipulating the vehicle's perceived position, potentially causing erroneous distance-keeping or inappropriate reactions to other vehicles.

Velocity Attacks: These attacks alter the vehicle's velocity data, leading to sudden accelerations or decelerations that could disrupt the flow of traffic.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017

Acceleration Attacks: In this scenario, the vehicle's acceleration or deceleration rates are manipulated, affecting the smoothness of the traffic flow and potentially leading to instability in the platoon.

Each of these cyberattacks is simulated across the different vehicle types classified by their size (small, medium, large). The classification takes into account the assumption that larger vehicles require greater safety headways and have lower maximum acceleration, deceleration, and velocity capabilities.

4.3 Simulation Execution

The simulation is executed under various scenarios to evaluate how the introduction of cyberattacks affects the overall traffic flow and the behavior of individual vehicles. The focus is on the longitudinal dynamics of the CAV platoon, including parameters such as headway distance, velocity profiles, and platoon stability. By systematically varying the type of cyberattack and the characteristics of the vehicles involved, the simulation captures a wide range of potential outcomes.

4.4 Data Analysis and Evaluation

Once the simulations are completed, the resulting data is analyzed to assess the impact of cyberattacks on traffic flow. Key metrics include the stability of the CAV platoon, changes in traffic density, and the occurrence of any traffic disturbances or accidents. The results are then compared across different vehicle types to determine how size and dynamic capabilities influence the resilience of the traffic flow to cyberattacks.

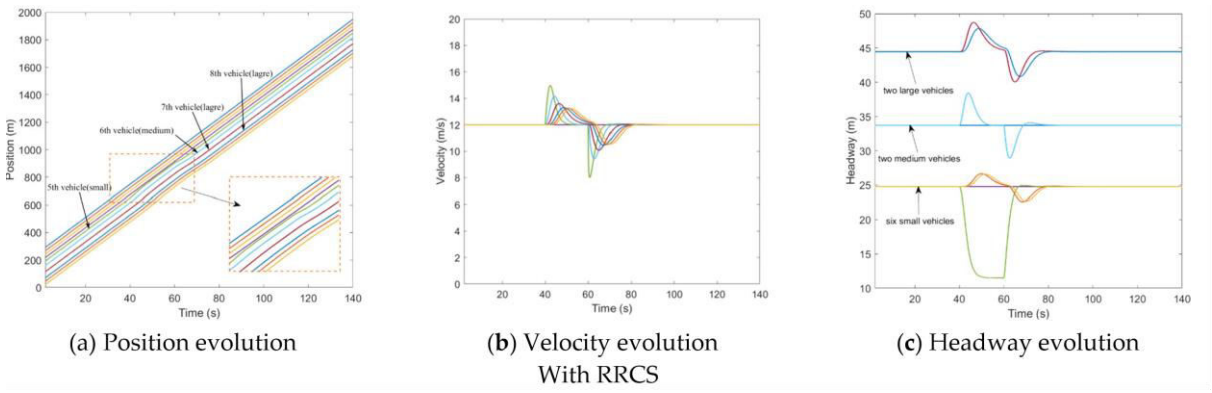
The analysis also considers the broader implications of these findings for CAV system design and cybersecurity measures. By identifying which types of vehicles and cyberattacks have the most significant impact on traffic flow, the study provides insights into how future CAV systems can be better protected against cyber threats, thereby enhancing overall traffic safety.

V. RESULT AND DISCUSSION

Table 1: Parameter values of different types of vehicles

Parameter	l	v_0	a	b	T	τ	s_0	T_g	T_u	a_{cmax}	d_{emax}
Unit	m	m/s	m/s^2	m/s^2	s	s	m	s	s	m/s^2	m/s^2
Small vehicle	5	33	2.5	3	1.3	0.1	4	1.3	3.5	2.5	4
Medium vehicle	8	27	2	2	1.6	0.15	6	1.6	3.8	2	3
Large vehicle	11	22	1.5	1	2	0.2	8	2	4	1.5	2

This section presents and analyzes the results of numerical simulations conducted to assess the impact of cyberattacks on mixed CAV traffic flow, specifically focusing on the effects of bogus velocity messages that either overestimate or underestimate the actual vehicle velocity. The simulations compare traffic flow dynamics both with and without the application of a Resilient Remote Control Strategy (RRCS), providing insights into the efficacy of RRCS in mitigating the adverse effects of cyberattacks.

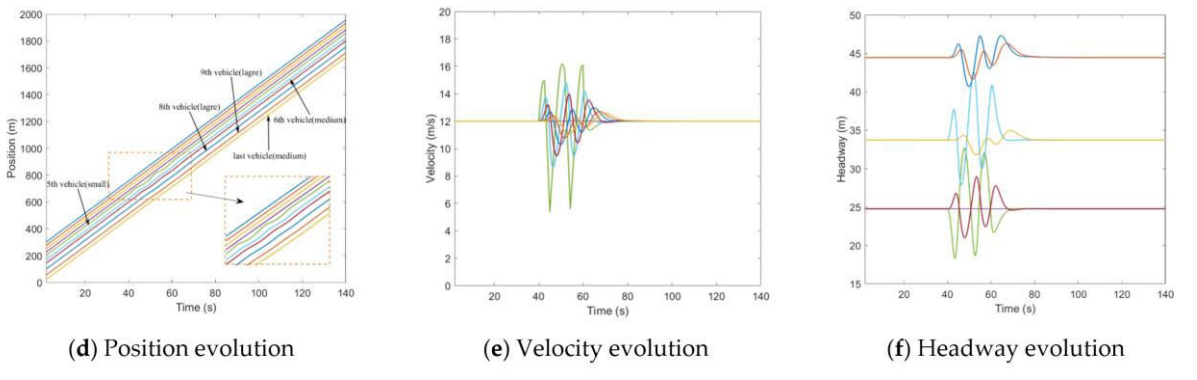


(a) Position evolution (b) Velocity evolution With RRCS (c) Headway evolution

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017



(**d**) Position evolution (**e**) Velocity evolution (**f**) Headway evolution

Figure 3: Diagrams illustrating the evolution of mixed traffic flow under the influence of overestimated velocity messages, comparing scenarios with and without RRCS.

5.1 Impact of Overestimated Velocity Messages

In the first scenario, a cyberattack was simulated where the fourth vehicle in the CAV platoon transmitted overestimated velocity information (1.5 times the actual velocity) to the fifth vehicle between t = 40s and t = 60s. The analysis of traffic flow without the RRCS (Figures 3a–c) revealed that the fifth vehicle, receiving the falsified higher velocity data, continued to accelerate in an attempt to close the perceived gap with the vehicle in front. This acceleration increased the risk of a potential collision as the vehicle failed to maintain a safe following distance. However, after the cyberattack ended at t = 60s, the traffic flow gradually returned to a stable state, but not without having posed significant safety hazards during the attack period.

When RRCS was applied (Figures 3d–f), the results demonstrated a marked improvement in the safety and stability of the CAV platoon under the same attack conditions. The fifth vehicle, despite receiving the overestimated velocity message, maintained a safe distance from the fourth vehicle, thereby mitigating the risk of collision. The evolution of velocity and headway under RRCS (Figure 3f) showed that the vehicles were able to maintain consistent inter-vehicle distances, even during the attack. This stability allowed the platoon to recover quickly once the cyberattack ceased, demonstrating that RRCS effectively enhances the resilience of CAV systems against overestimated velocity attacks. The ability of RRCS to maintain traffic stability and safety under these adverse conditions underscores its potential as a vital tool for CAV cybersecurity.

5.2 Impact of Underestimated Velocity Messages

In the second scenario, the cyberattack involved tampering with the fourth vehicle's velocity data to transmit a value that was only 40% of the actual velocity. This resulted in the fifth vehicle underestimating the speed of the vehicle ahead, leading to unnecessary deceleration between t = 40s and t = 60s. Without the RRCS (Figures 4a–c), the fifth vehicle's deceleration created a larger-than-necessary headway, which, while not immediately dangerous, represented an inefficient use of road space and contributed to potential traffic congestion. The increased spacing between vehicles could lead to a reduced road capacity and slower traffic flow, thus wasting valuable transportation resources.

In contrast, the application of RRCS (Figures 4d–f) significantly mitigated the negative impact of the underestimated velocity attack. The fifth vehicle, despite receiving incorrect velocity data, was able to maintain a more appropriate speed and headway. The simulations showed that RRCS effectively reduced the fluctuations in velocity and minimized unnecessary increases in headway. This ensured that the platoon remained stable and that road resources were utilized more efficiently, even under attack. The ability of RRCS to counteract the effects of underestimated velocity messages further demonstrates its effectiveness in maintaining the operational integrity of CAV systems in the face of cyber threats.

5.3 Comparative Analysis and Implications

Comparing the effects of the two types of cyberattacks, it is evident that overestimating velocity poses a more immediate safety risk due to the potential for collisions, whereas underestimating velocity primarily affects traffic efficiency and road capacity. The results highlight the critical role of accurate velocity information in maintaining both the safety and efficiency of CAV operations.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017

The application of RRCS in both scenarios proved to be highly effective in mitigating the adverse effects of cyberattacks. By maintaining appropriate vehicle spacing and stability, RRCS not only enhances the safety of the CAV platoon but also optimizes traffic flow, ensuring that road resources are not wasted due to unnecessary decelerations or accelerations.

These findings have important implications for the development and deployment of CAV systems. First, they emphasize the need for robust cybersecurity measures, such as RRCS, to protect CAV systems from potential cyberattacks that could compromise vehicle safety and traffic efficiency. Second, the results suggest that future CAV designs should incorporate mechanisms that can detect and counteract the effects of falsified velocity information, ensuring that vehicles can respond appropriately even when under attack.

The numerical simulations demonstrate the significant impact that cyberattacks can have on mixed CAV traffic flow, particularly when vehicles are not equipped with protective measures like RRCS. The effectiveness of RRCS in maintaining traffic stability and safety under attack conditions highlights its potential as a critical component of future CAV systems, contributing to safer and more efficient road networks.

VI. CONCLUSION

The study provides a comprehensive analysis of the impact of cyberattacks on the dynamics of mixed Connected Automated Vehicle (CAV) traffic flow, with a particular focus on the effects of tampered velocity information. Through numerical simulations, the research has demonstrated that cyberattacks, such as overestimating or underestimating vehicle velocity, can significantly disrupt traffic flow and pose serious safety risks. These attacks can lead to dangerous situations, such as reduced following distances that increase the risk of collisions, or unnecessarily large headways that waste road capacity and hinder traffic efficiency.

A key finding of this study is the effectiveness of the Resilient Remote Control Strategy (RRCS) in mitigating these adverse effects. The application of RRCS across different attack scenarios showed that it can maintain the stability of the CAV platoon, ensuring that vehicles adhere to safe and efficient operational parameters even when subjected to compromised data. The ability of RRCS to preserve traffic stability and safety underlines its potential as a vital cybersecurity measure for CAV systems.

This research highlights the critical importance of robust cybersecurity frameworks in the future development and deployment of CAV technologies. As CAV systems become more prevalent, the threat of cyberattacks targeting vehicle dynamics will likely increase, necessitating the integration of effective defensive strategies like RRCS. Additionally, the study emphasizes the need for ongoing research to explore other potential vulnerabilities within CAV networks and develop comprehensive solutions to safeguard against a wide range of cyber threats.

In conclusion, the findings of this study underscore the dual necessity of enhancing both the technological capabilities and the cybersecurity resilience of CAV systems to ensure the safe and efficient operation of future transportation networks. Implementing strategies like RRCS will be crucial in protecting CAVs from cyberattacks and in realizing the full potential of connected and automated transportation systems.

REFERENCES

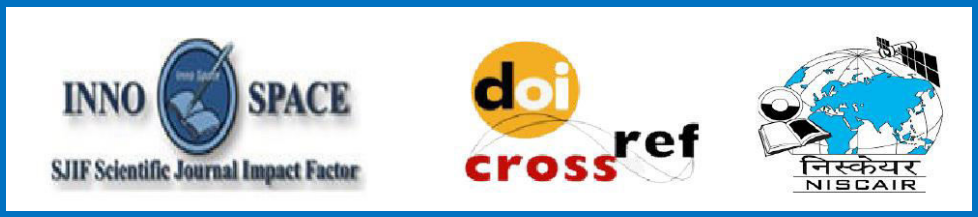
1. Zhao, L.; Sun, J. Simulation Framework for Vehicle Platooning and Car-following Behaviors Under Connected-vehicle Environ- ment. Procedia Soc. Behav. Sci. 2013, 96, 914–924.
2. Li, L.; Wen, D.; Yao, D. A Survey of Traffic Control With Vehicular Communications. IEEE Trans. Intell. Transp. Syst. 2013, 15, 425–432.
3. Rios-Torres, J.; Malikopoulos, A.A. A Survey on the Coordination of Connected and Automated Vehicles at Intersections and Merging at Highway On-Ramps. IEEE Trans. Intell. Transp. Syst. 2016, 18, 1066–1077.
4. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2898–2915.
5. Amir, A.; Monireh, D.; Zhang, H.; Zeng, K. String stability analysis of cooperative adaptive cruise control under jamming attacks. In Proceedings of the 18th International Symposium on High Assurance Systems Engineering (HASE), Singapore, 12–14 January 2017; pp. 157–162.
6. Wang, P.; Yu, G.; Wu, X.; Qin, H.; Wang, Y. An extended car-following model to describe connected traffic dynamics under cyberattacks. Phys. A Stat. Mech. Its Appl. 2018, 496, 351–370.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 3.361| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 6, Issue 5, September-October 2019 ||

DOI:10.15680/IJARETY.2019.0605017

7. Li, Y.; Tu, Y.; Fan, Q.; Dong, C.; Wang, W. Influence of cyber-attacks on longitudinal safety of connected and automated vehicles. Accid. Anal. Prev. 2018, 121, 148–156. [PubMed]
8. S. Senthilkumar, L. Ramachandran, R. S. Aarthi, "Pick and place of Robotic Vehicle by using an Arm based Solar tracking system", International Journal of Advanced Engineering Research and Science, vol. 1, no. 7, pp. 39-43, 2014.
9. D. Nathangashree, L. Ramachandran, S. Senthilkumar & R. Lakshmirekha, "PLC based smart monitoring system for photovoltaic panel using GSM technology", International Journal of Advanced Research in Electronics and Communication Engineering, vol. 5, no. 2, pp.251-255, 2016.
10. Senthilkumar. S, Lakshmi Rekha, Ramachandran. L & Dhivya. S, "Design and Implementation of secured wireless communication using Raspberry Pi", International Research Journal of Engineering and Technology, vol. 3, no. 2, pp. 1015-1018, 2016.
11. A. Renuka Devi, S. Senthilkumar, L. Ramachandran, "Circularly Polarized Dualband Switched-Beam Antenna Array for GNSS" International Journal of Advanced Engineering Research and Science, vol. 2, no. 1, pp. 6-9; 2015.
12. Raya, M.; Hubaux, J.-P. Securing vehicular ad hoc networks. J. Comput. Secur. 2007, 15, 39–68. [CrossRef]
13. Cui, J.; Liew, L.S.; Sabaliauskaite, G.; Zhou, F. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Netw. 2018, 90, 101823. [CrossRef]
14. Khattak, Z.H.; Park, H.; Hong, S.; Boateng, R.A.; Smith, B.L. Investigating Cybersecurity Issues in Active Traffic Management Systems. Transp. Res. Rec. J. Transp. Res. Board 2018, 2672, 79–90. [CrossRef]
15. Zeadally, S.; Hunt, R.; Chen, Y.-S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. Telecommun. Syst. 2010, 50, 217–241. [CrossRef]



International Journal of Advanced Research in Education and TechnologY (IJARETY)

www.ijarety.in editor.ijarety@gmail.com