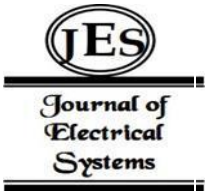
[1]Mrs. B. Hidayathunisa

[2]Dr. A. Shaik Abdul Khader

System Response Topology for the Anomalies (SysRTA) using Ideology Based-Deep Reinforcement Learning (IB-DRL) in Intelligent Transport System



Abstract: - An Intelligent Transport System (ITS) is a comprehensive technological solution designed to enhance the efficiency, safety, and sustainability of transportation networks. Leveraging a range of information and communication technologies, ITS aims to manage and optimize traffic flow, enhance transportation safety, reduce congestion, and enhance overall mobility. This paper proposed System Response Topology for the Anomalies (SysRTA) using Ideology Based-Deep Reinforcement Learning (IB-DRL). SysRTA-ID-DRL algorithm proposes. Dynamic Speed Harmonisation (DSH) is a component of the proposed algorithm. It has potential for reducing traffic fluctuations during periods of congestion. However, because of drivers' low adherence rates and long access times to information, its effectiveness frequently encounters limitations. Intelligent transport systems attempt to improve in a number of ways by integrating connected and automated vehicles (CAVs).This approach involves calibrating the Multiple Vehicle Intelligent Driver Model (IDM) and subsequently employing the actual dataset HISTORIC for training the trajectory prediction model. IB-DRL is under development to explore the ways in which Connected and Automated Vehicles (CAVs) can improve operational performance. A thorough analysis is conducted to measure the impacts of multiple simulated scenarios, each featuring different levels of CAV adoption.

Keywords: Intelligent Transport System (ITS), Dynamic Speed Harmonisation (DSH), fluctuations

Introduction

CAVs, or connected and automated vehicles, are a game-changing advancement in the transportation industry. These vehicles use cutting-edge technology to increase on-road mobility, safety, and efficiency. An overview of linked and automated automobiles is provided below:

Nodes with connections:

Vehicle-to-Vehicle (V2V) Communication: Via wireless technology, connected cars can connect with one another and exchange information about their location, speed, and other pertinent factors. This makes it easier to detect probable collisions and dangerous driving situations early on, which helps prevent accidents.

Communication between connected automobiles and various infrastructure components, such as traffic signals, road signs, and highway sensors, is known as "vehicle-to-infrastructure" (V2I) communication. This connectivity enables traffic management systems to inform drivers in real-time about the state of the road, thereby improving traffic flow.

Data sharing: Connected vehicles produce and send data to traffic management facilities, providing information on the state of the roads, traffic jams, and other relevant concerns. Utilising this data can help with better traffic management and incident response.

Better Navigation: Through connectivity, vehicles may get the most recent navigation data and updates, empowering drivers to choose the best routes and avoid traffic with knowledge.

Autonomous Vehicles

Levels of Automation: Automated vehicles are frequently divided into different automation levels, ranging from Level 0 (complete lack of automation) to Level 5 (full automation). These ratings show how much of a vehicle

[1]Research scholar, PG & Research Department of Computer Science, Khadir Mohideen College (Autonomous), Adirampattinam-614701,(Affiliated to Bharathidasan University, Tiruchirappalli-620024), Tamilnadu, India

E-mail: hima_mca@yahoo.co.in

[2]Research supervisor, PG & Research Department of Computer Science, Khadir Mohideen College (Autonomous), Adirampattinam-614701, (Affiliated to Bharathidasan University, Tiruchirappalli-620024), Tamilnadu, India

E-mail: hiqmath4u@gmail.com

can run without human involvement. For instance, Level 1 could include functions like adaptive cruise control, whereas Level 4 denotes a vehicle's ability to handle every aspect of driving in a given situation.

Automated cars use a variety of sensors, such as lidar, radar, cameras, and ultrasonic sensors, to sense their environment. For the purpose of making knowledgeable decisions about vehicle control, sophisticated software analyses this sensor data.

Control Systems: Automated vehicles use cutting-edge control systems to decide when to steer, accelerate, and brake. These systems run on algorithms that take sensor and map data into account.

Safety and testing: It is crucial to ensure the safety of automated vehicles. To reduce the risk of system failures, rigorous testing and validation processes are used, incorporating redundancy measures. Additionally, efforts are being made to create safety standards and guidelines specifically for automated cars.

Impact on the Environment and Traffic: By enhancing driving habits, automated vehicles have the potential to improve fuel economy and cut emissions. By facilitating techniques like platooning, in which cars move closely together at a constant pace, they can also reduce traffic congestion.

Problems & Moral Issues: The development and adoption of connected and automated vehicles (CAVs) raise ethical and legal concerns, including those relating to data privacy, accident responsibility, and the future eviction of professional drivers.

Especially for those with impairments or restricted access to conventional transportation, connected and automated cars have the potential to revolutionise transportation by improving safety, reducing traffic, and enhancing mobility options. However, the widespread use of CAVs poses complex issues that need for serious analysis and action from manufacturers, governments, and society at large.

The future vision of mobility is expected to feature Connected and Automated Vehicles (CAVs), which are distinguished by their wireless communication capabilities. CAVs are poised to address the growing demand for mobility while mitigating the associated negative environmental and social consequences. Through wireless connectivity, these vehicles will autonomously create platoons, traveling closely together to conserve fuel, reduce accident risks, and open up additional lanes to alleviate traffic congestion [3, 4]. However, the open communication environment also exposes CAVs to various cybersecurity threats such as fabrication, eavesdropping, flooding, and replay attacks, posing significant risks to traffic efficiency and driver safety. As a result, the implementation of an adaptive response system becomes crucial when vehicles come under cyberattacks.

Review of Literature

It is commonly acknowledged that there are currently no real-world deployments of Dynamic Speed Harmonisation (DSH) systems based on Connected and Automated Vehicles (CAVs), and only a small number of institutions have the facilities required for carrying out field tests. As a result, many research use simulation-based techniques, which can be divided into two categories: reactive and proactive. Once congestion is identified, reactive solutions comprise turning on the Variable Speed Limit (VSL) controller [1]. These techniques, which can be used in stationary traffic scenarios, rely on offline algorithms that have their roots in classical feedback control theory. However, they frequently have congestion management delays, and therefore need basic traffic diagrams to adjust controller settings. Proactive approaches have been suggested to address this problem, seeking to predict future traffic patterns and take necessary action before congestion develops [2]. We explore the VSL algorithms within DSH tactics in the subsections that follow, with an emphasis on CAVs and other intelligent vehicles in particular.

Wang et al. [3] objective was to establish a modeling framework aimed at enabling a comprehensive assessment of Cyber-Attacks' impacts on Connected and Automated Vehicles (CAVs). Wang introduced the Cooperative Intelligent Driver Model (CIDM) in detail, and numerical experiments demonstrated that various cyberattacks could lead to unintended consequences such as delayed responses, very narrow following distances, sudden accelerations or decelerations, and even rear-end collisions among vehicles. Examining the influence of minor cyberattacks on CAVs' longitudinal security, Li et al. [4] conducted research. Cheng and team [5] developed an innovative intelligent driving model that accounted for cyberattacks and heterogeneous vehicle compositions.

Their work revealed that the impact of a cyberattack on heterogeneous platoons surpasses that on homogeneous platoons and that higher car penetration rates enhance traffic flow stability. Dong et al. [6] designed an assessment framework that offers a comprehensive evaluation of transportation systems within the context of IET Intell. This framework was created to assess the impact of cyberattacks across various dimensions, including effectiveness, safety, emissions, and fuel consumption.

The aforementioned study thoroughly evaluated transportation networks, emphasising network security. Khattak et al.'s study [8] examined the various effects of three different kinds of cyberattacks on traffic safety and stability in an environment with numerous Connected and Autonomous Vehicles (CAVs) and lane changes. Sun and colleagues [9] conducted additional research that included testing time-delay and disturbance attacks on unsignalized intersections and motorway segments, respectively. To evaluate the effects of cyberattacks on transport systems, they used a variety of efficiency and safety metrics.

As previously discussed, the mentioned studies primarily concentrate on assessing the detrimental effects of cyberattacks, emphasizing their negative consequences. However, these studies overlook the critical aspect of designing control systems capable of handling cyberattacks and ensuring traffic safety. Building upon earlier research [10], various control strategies have been identified to mitigate the adverse impacts of cyberattacks, falling into five distinct categories: observer-based control strategy [11, 12], robust control strategy [10, 13], adaptive control strategy [14, 15], model predictive control (MPC) strategy [16, 17], and deep reinforcement learning control (DRL) strategy [18, 19].

Each control strategy possesses unique characteristics. For instance, the observer-based control strategy ensures platoon stability by utilizing radar information and wireless communication to detect and isolate cyberattacks. The adaptive control strategy maintains the boundedness of the closed-loop system by dynamically adjusting controller parameters, effectively countering the influence of false information. Notably, model predictive control (MPC), recognized as an advanced method for controlling processes while adhering to constraints, is prominently featured in this context. Wang et al. [16] proposed a dynamic output feedback approach to address deception attacks, while Lyu et al. [17] devised a communication topology safety response system coupled with distributed model predictive control for connected and automated truck platoons facing cyber threats. Numerical results underscore the feasibility of these control strategies in resisting cyberattack threats.

However, current research on cyberattack response control strategies has certain limitations. Firstly, it overlooks the response strategies of Cooperative Adaptive Cruise Control (CAVP) in the presence of cyberattacks involving multiple vehicles. Secondly, it assumes that the expected reference trajectory in the response control module under cyberattack scenarios is predefined and known, which does not align with real-world conditions

Proposed System

The System Response Topology for the Anomalies (SysRTA) Architecture

In order reduce the impact of cyberattacks, a "System Response Topology for the Anomalies" is presented in this section. Within the CAVP domain, vehicle functionality is heavily reliant on V2V communication, with radar data serving as a backup to ensure reliable and robust performance. The trigger module and the control module, the two main parts of SysRTA, are shown in the diagram as the organization's structure. The following is an outline of the SysRTA's thorough operational method.

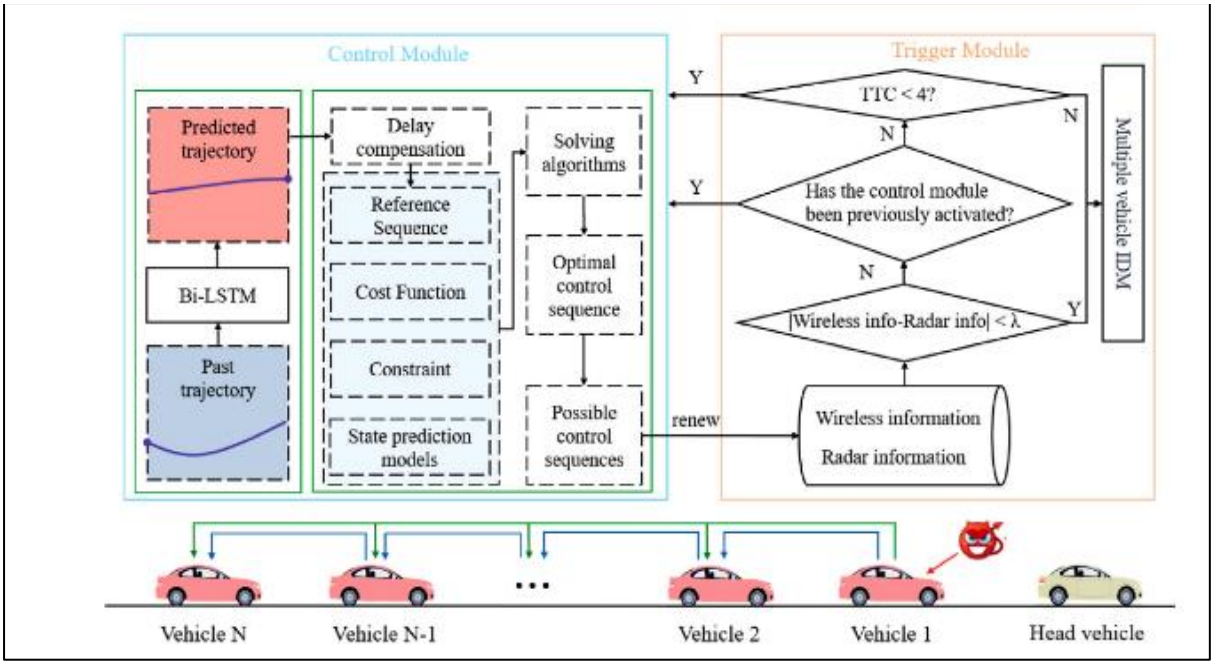


Figure 1. The architecture of SysRTA

In the Trigger module, real-time distance data from radar detection and V2V are evaluated. The first calculation is determining whether the difference in the two distance values is greater than 0.5 m. The vehicle remains under the original multiple vehicle IDM management if the variance is less than the threshold. The system determines whether the SysRTA-ID-DRL control module is already turned on if the deviation is greater than the threshold. It is maintained if it is triggered; if not, it moves on to the second assessment, which determines whether the Time-to-Collision (TTC) determined from radar data exceeds a predetermined threshold. The vehicle retains the multiple vehicle IDM mode for driving when the TTC exceeds 4 seconds; otherwise, the SysRTA-ID-DRL control module is triggered when the TTC is less than 4 seconds. New real-time vehicle data is sent to the triggering module for a new round of deliberation and decision-making after every time step.

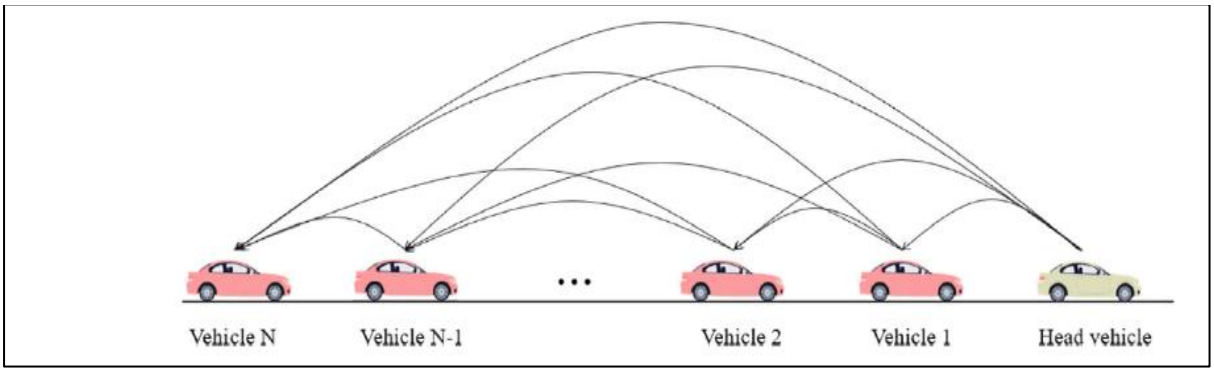


Figure 2 The information flow topology of CAVP without cyberattack

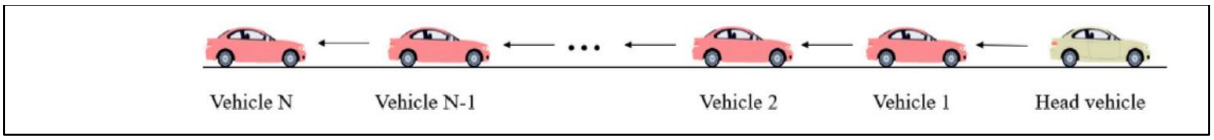


Figure 3: The information flow topology of CAVP with cyberattack

It is significant that radar data is prioritised over wireless data for platoon control in the event of a cyberattack on SysRTA. The information flow topology changes to Figure 3 and V2V information is ignored. Naturally, the information flow topology returns to the mode shown in Figure 1 after the cyberattack has been stopped. The Time-to-Collision (TTC) indicator is used to measure the risk of a rear-end collision and determine the security level [7]. It is computed using the formula below:

$$T'\Gamma C_i(t) = \{\frac{x_{i-1}(t) - x_i(t) - l_{i-1}}{v_i(t) - v_{i-1}(t)},\ if\ v_i(t) > v_{i-1}(t)\ \infty\ ,\ if\ v_i(t) \le v_{i-1}(t)\ ,$$

The positions of the vehicles that come before and after are indicated by the symbols $x_{i-1}(t)$ and $x_i(t)$, respectively. The length of the previous vehicle is indicated by li−1, and the velocities of the next and previous vehicles are indicated by $v_i(t)$ and $v_{i-1}(t)$, respectively.

The SysRTA-ID-DRL structural design

In this section, SysRTA-ID-DRL is defined as the SysRTA control module. SysRTA-ID-DRL uses a unique method, in contrast to conventional Model Predictive Control (MPC) with preset reference trajectories. In particular, it uses the reference trajectory to be the anticipated speed of the vehicle ahead of it over a predetermined amount of time, as determined by ID-DRL [29, 30]. An important innovation is this SysRTA/ID-DRL integration.

Deep reinforcement learning framework of DRL

A key idea in Deep Reinforcement Learning (DRL) is the Markov decision process (MDP), which can be used to model the difficulty of the Downstream Highway (DSH) problem. Sets of states (S) and actions (A), transition probabilities (P) guided by a policy π, and immediate rewards (R) with a discount factor γ comprise the MDP, represented as (S, A, P, R). In this framework, the agent's goal is to maximise cumulative rewards by interacting with the surroundings.

Figure 4 illustrates how DRL is implemented in DSH. In this configuration, traffic parameters are received as the state from the downstream congestion area by the Virtual Speed Limit (VSL) controller, which acts as the agent under the supervision of a DRL algorithm. After that, the agent decides on variable speed limits and feeds those decisions back to the surroundings. A defined policy governs the environment, which generates a new state based on the previous state and action. By using performance indicators to represent cumulative rewards, the feedback loop seeks to maximise them.

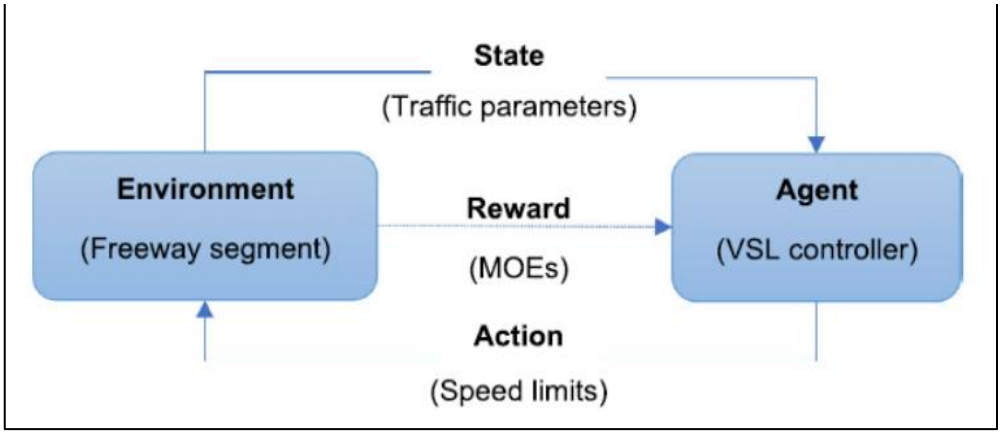


Figure 4. The control scheme of DRL in DSH

The environment (a highway mainline segment with a weaving area), the agent (a VSL controller), and the state, action, and reward functions are the main parts of the DRL system. The traffic states that are gathered by detectors and represent variables like density, average speed, or volume of traffic make up the state. The current occupancy rates of every lane in the downstream weaving area, on-ramp, and upstream mainline are all part of the state

dimension. The reward function prioritises safety and measures actions as differential speed limits for each lane, with cumulative emergency deceleration exceeding a predetermined threshold.

The DRL algorithm adjusts speed limits dynamically in response to different levels of traffic congestion in an effort to improve safety by controlling emergency deceleration. The study treats each Connected and Automated Vehicle (CAV) as a VSL controller and focuses on a single-agent system. The intricacy of solving the DSH problem with DRL is highlighted by the complex interactions that exist between state representation, action selection, and reward definition.

DRL controller algorithm of VSL

Deep Deterministic Policy Gradients, or DDPG, is the algorithm of choice for regulating the speed limit in the Deep Reinforcement Learning (DRL) framework [38]. Combining on-policy gradients and off-policy Q-learning, DDPG is a model-free algorithm. When discrete Q-learning is used in situations where each lane has a different speed limit, the action dimension can grow significantly, which could result in a space explosion issue. In order to overcome this difficulty, it is imperative to utilise an algorithm that can handle continuous actions without listing every possible value.

One notable feature of DDPG is its ability to handle continuous actions, which offers a great deal of flexibility when creating different Downstream Highway (DSH) strategies [37]. The algorithm functions within an actor-critic framework, wherein the same deep neural networks are used to approximate both value- and policy-based functions. After actions are chosen by the actor component, the critic assesses the policy π that the actor defined and forecasts the target Q-value function. With continuous action spaces and the requirement for nuanced strategies, DSH scenarios present significant challenges that can only be successfully navigated by DDPG thanks to this dual functionality.

$$Q(s,a) = r(s,a) + \gamma Q(s',a)$$

The actor's goal in the DDPG algorithm is to maximise the Q value predicted by the critic through trial-and-error interactions, where's' represents the current state,'s″ indicates the next state, 'r' indicates the reward function, and γ (the discount factor) is set to 0.9. Whereas the target policy for action is deterministic, DDPG uses a stochastic policy for action exploration. In a bi-level optimisation pattern, the actor's (θa) and critic's (θc) parameters are updated during the optimisation process.

To reduce its loss—which is the difference between the two sides of the Bellman equation—the critic applies the Adam optimizer. Based on the gradients in the loss functions L(Q, θc) and L(π, θa), respectively, the weights of θc and θa are updated. The temporal difference error serves as a guide for this update process, making sure that the actor and critic parameters change over time to increase the precision of Q value predictions and the actor's policy in the given environment.

$$\theta^c = argmin_{\theta^c} Q_{\theta c}(s,a) - \left(r(s,a) + Q_{\theta c}\left(s', \pi(s')\right)\right)$$

$$L(Q,\theta^c) = \frac{\sum_1^N (\theta^c)^2}{N_{sample}} L(\pi,\theta^a) = -\frac{\sum_1^N Q^{(s,\pi_{\theta^a}(s))}}{N_{sample}}$$

The deterministic policy gradient is used to update θa's parameters.

$$\nabla_{\theta^a} = \frac{1}{N_{sample}} \sum_1^N \nabla_a Q_{\theta^c}(s,a)|_{a=\pi_{\theta^a}(s)} \nabla_{\theta^a} \pi_{\theta^a}(s)$$

With parameter τ set to 0.01 and a soft update mechanism, the target actor and critic models are replaced in a smooth manner. Experience replay is used to improve learning efficiency by sifting through 30,000 experiences in a replay memory to save important ones and discarding less valuable ones. For the actor and critic in this study, lightweight neural networks with two layers of thirty neurons each are used. The learning rate for the actor and critic is set to 0.0001 and 0.0002, respectively, for a batch size of 32. To dynamically modify the learning rates for every neural network weight, the Adam optimizer is utilised. The following can be used to express the representations of critic C and actor A:

$$h_t^a = relu(W_1^a + b_1^a)$$

$$a_t = A * sigmoid^a(W_2^a b_t^a + b_2^a)$$

$$b_t^c = relu(W_s^c s_t + W_a^c a_t + b_1^c)$$

$$Q_t = W_2^c b_t^c + b_2^c$$

Each model's network parameters are set with a state dimension (S) of 10 and an action dimension (A) of 6.

$$W_1^a, W_s^c \in R^{30*10}, W_2^a, W_2^c \in R^{1*30}, b_1^a, b_1^c \in R^{30}, b_2^a, b_2^c \in R^1$$

relu and sigmoid are the activation functions that are used. In this study, every hyperparameter was adjusted over several iterations. The following is a brief summary of the DDPG algorithm's steps for Downstream Highway (DSH):

Step 1 involves initializing parameters and defining target weights for both the actor network θa and the critic network θc. Subsequently, the replay buffer is cleared.

Step 2, the environment is loaded, and the current state 's' is observed. Steps 2 to 6 are iteratively repeated until the episode reaches its maximum.

Step 3, throughout the simulation's time steps, actions 'a' are explored based on the current policy π, and the noise decay is implemented during execution.

Step 4 involves selecting variable speed limits, receiving the corresponding reward 'r', and obtaining the new state 's′'. This Markov Decision Process (MDP) is then stored in the replay buffer.

Step 5, a batch of transitions is randomly sampled from the replay buffer, and the target function Q is computed.

Step 6, the Q function is updated by minimizing the loss L(Q, θc), and simultaneously, the policy is updated using the deterministic policy gradient ∇θa.

Step 7, the target actor θa and critic θc networks undergo updates using a soft replacement strategy, expressed as $\tau\theta$a + (1 − τ)a and $\tau\theta$c + (1 − τ)θc, until convergence is achieved.

Simulation Parameters

Table 1. Simulation Parameter

Parameter Type	**Symbol**	**Value**
Simulation Time	-	160s
operation	-	10Hz
Max acceleration	d_{max}	0.7099 m⁄s^2
Max comfortable deceleration	b	3.1125 m⁄s^2
Desired velocity	v_0	30 m/s
Jam distance	s_0	6m
Desired time headway	T	1.8224s
Weight factor	$\alpha_{n,n-1}$	0.7937
Weight factor	$\alpha_{n,n-2}$	0.2063
Number of preceding vehicles for communication	M	2

Result and Discussion under collusion attacks

In this situation, a cyberattack occurs between t = 40s and t = 120s, involving a coordinated cyberattack where information from multiple vehicles is tampered with and transmitted. More specifically, the transmission speed

information of vehicle 1 is maliciously altered to be 25 meters higher than the true value, with the reported velocity being 1.5 times the actual value. This same level of attack intensity is simultaneously applied to vehicle 3.

In the absence of SysRTA communication range limiting the two vehicles affected by the collusion cyberattack, all vehicles, excluding Vehicle 1, depend on the manipulated information. As a consequence, these vehicles incorrectly perceive the leading vehicle as accelerating, leading to a mistaken belief that the distance between vehicles is expanding.

Table 2. The 1⁄TTC distribution under collusion cyberattacks without SysRTA; with SysRTA.

1/TTC	Without SysRTA-ID-DRL	With SysRTA-ID-DRL
0.06	58	25
0.07	50	12
0.08	36	13
0.09	41	8
0.1	28	12
0.11	15	11
0.12	9	10
0.13	8	9
0.14	8	9
0.15	7	10
0.16	7	6
0.17	7	9
0.18	6	6
0.19	6	8
0.2	5	7
0.21	5	6
0.22	5	9
0.23	5	6
0.24	5	7
0.25	4	40

Figure 5 illustrates a comparison of the distribution of 1/TTC under collusion attacks with and without SysRTA. The data presented in Figure 14 leads to two noteworthy conclusions. Firstly, the frequencies corresponding to $0 \leq 1/TTC \leq 0.1$, $0.1 < 1/TTC < 0.25$, and $1/TTC \geq 0.25$ are 2087, 76, and 1453, constituting 57.71%, 40.18%, and 0.0211%, respectively. It is important to highlight that the implementation of SysRTA results in a 39.22% improvement in the safety of the Connected and Automated Vehicle Platoon (CAVP) based on the criterion of $1/TTC \leq 0.25$.

Secondly, a significant observation is that the risk posed to the CAVP during collusion cyberattacks is higher compared to bogus cyberattacks. This is evident in the fact that the frequency ratio of $1/TTC \geq 0.25$ has increased from 28.98% to 40.18%.

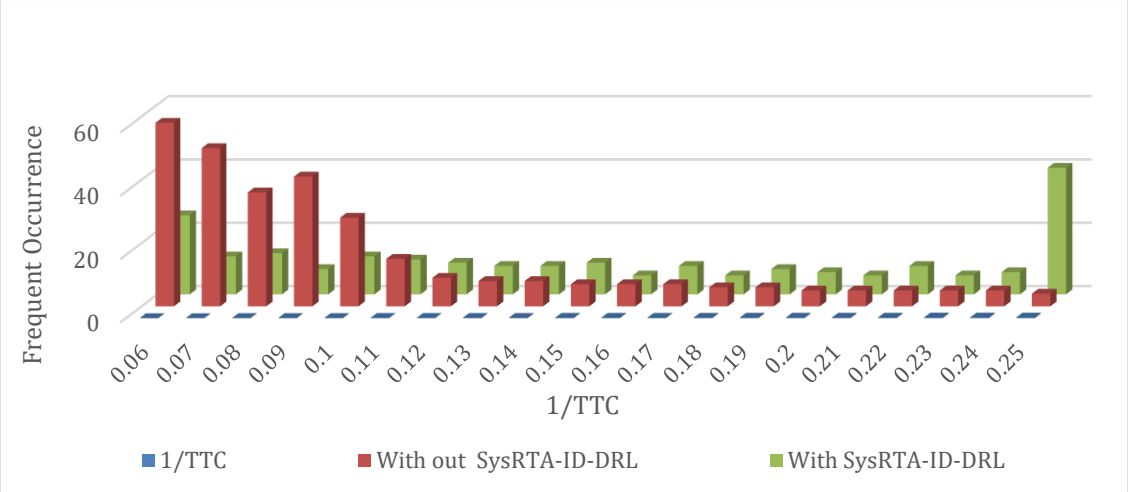


Figure 5. The 1⁄TTC distribution under collusion cyberattacks without SysRTA; with SysRTA.

Conclusion

The widespread integration of autonomous driving technology brings numerous advantages, but it also raises concerns about the substantial cybersecurity risks faced by Connected and Automated Vehicle Platoon (CAVP). Addressing these concerns, this paper initiates exploratory efforts to develop a dedicated cyberattack response system tailored specifically for CAVP. To begin, a multiple car-following model is calibrated to represent the CAVP environment. Furthermore, a System Response Topology for Anomalies (SysRTA) is introduced, comprising a trigger module and a control module. The paper concludes by conducting numerical experiments on CAVP evolution in cyberattack scenarios, using the simulation of driving behavior based on processed real dataset HISTORIC to validate the effectiveness and feasibility of the proposed SysRTA.

Key findings of the paper include:

Cyberattacks exert significant and detrimental impacts on the stability and security of CAVP, with rear-end collisions particularly affected. Collusion attacks, involving multiple CAVs, emerge as the most potent threat, exerting the highest negative influence on CAVP stability and security.

The proposed SysRTA effectively mitigates the adverse effects of cyberattacks, demonstrating excellent performance in responding to such threats. Its resilience is attributed to dynamic communication topology switching using triggering modules and the utilization of the control module based on SysRTA-ID-DRL to counter cyberattack threats.

While the paper provides valuable insights, there are areas for further exploration. For instance, future research could integrate more multi-source sensor data to design more effective control strategies for combating cyberattacks.

References

[1]. Malikopoulos, A.A., Hong, S., Brian Park, B., Lee, J., Ryu, S.: Optimal control for speed harmonization of automated vehicles. IEEE Trans. Intell. Transp. Syst. 20(7), 2405–2417 (2019). https://doi.org/10.1109/tits.2018. 2865561

[2]. Khondaker, B., Kattan, L.: Variable speed limit: an overview. Transp. Lett.7(5), 264–278 (2015). https://doi.org/10.1179/1942787514y.0000000053

[3]. Wang, P., Wu, X., He, X.: Modeling and analyzing cyberattack effects on connected automated vehicular platoons. Transp. Res. Part C: Emerg. Technol. 115, 102625 (2020)

[4]. 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. 121, 148–156 (2018)

[5]. Cheng, R., Lyu, H., Zheng, Y., Ge, H.: Modeling and stability analysis of cyberattack effects on heterogeneous intelligent traffic flow. Physica A 604, 127941 (2022)

[6]. Dong, C., Wang, H., Ni, D., Liu, Y., Chen, Q.: Impact evaluation of cyberattacks on traffic flow of connected and automated vehicles. IEEE Access 8, 86824–86835 (2020)

[7]. Zhang, L., Liu, H., Sun, J., Wang, D.: Variable speed limit strategy to improve the safety and environmental impact of freeway traffic. Paper presented at the Transportation Research Board 94th Annual Meeting, Washington DC, United States, 11–15 January 2015 (2015). https://trid.trb.org/view/1338666

[8]. Khattak, Z.H., Smith, B.L., Fontaine, M.D.: Impact of cyberattacks on safety and stability of connected and automated vehicle platoons under lane changes. Accid. Anal. Prev. 150, 105861 (2021)

[9]. Sun, Z., Liu, R., Hu, H., Liu, D., Yan, Z.: Cyberattacks on connected and automated vehicles: A traffic impact analysis. IET Intel. Transport Syst. 1–17 (2022)

[10]. Zhou, A., Wang, J., Peeta, S.: Robust control strategy for platoon of connected and autonomous vehicles considering falsified information injected through communication links. J. Intell. Transp. Syst. 1–17 (2022)

[11]. Merco, R., Biron, Z.A., Pisu, P.: Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control. In: 2018 Annual American Control Conference (ACC), pp. 5582–5587. IEEE, Piscataway (2018)

[12]. Kremer, P., Koley, I., Dey, S., Park, S.: State estimation for attack detection in vehicle platoon using VANET and controller model. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), pp. 1–8. IEEE, Piscataway (2020)

[13]. Zheng, Y., Li, S.E., Li, K., Ren, W.: Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed H-infinity controller synthesis. IEEE Trans. Intell. Transp. Syst. 19(5), 1353–1364 (2018)

[14]. Jin, X., Haddad, W.M., Jiang, Z., Kanellopoulos, A., Vamvoudakis, K.G.: An adaptive learning and control architecture for mitigating sensor and actuator attacks in connected autonomous vehicle platoons. Int. J. Adapt. Control Signal Process. 33(12), 1788–1802 (2019)

[15]. Yadegar, M.,Meskin,N., Haddad,W.M.: An output-feedback adaptive control architecture for mitigating actuator attacks in cyber-physical systems. Int. J. Adapt. Control Signal Process. 33(6), 943–955 (2019)

[16]. Wang, J., Ding, B., Hu, J.: Security control for LPV system with deception attacks viamodel predictive control: A dynamic output feedback approach. IEEE Trans. Autom. Control 66(2), 760–767 (2021)

[17]. Lyu, H., Wang, T., Cheng, R., Ge, H.: Improved longitudinal control strategy for connected and automated truck platoon against cyberattacks. IET Intel. Transport Syst. 16(12), 1710–1725 (2022)

[18]. Ferdowsi, A., Challita, U., Saad, W., Mandayam, N.B.: Robust deep reinforcement learning for security and safety in autonomous vehicle systems. In: 2018 21st International Conference on Intelligent Transportation Systems (ITSC), pp. 307–312. IEEE, Piscataway (2018)

[19]. Lütjens, B., Everett, M., How, J.P.: Certified adversarial robustness for deep reinforcement learning. In: Conference on Robot Learning, pp. 1328–1337. IEEE, Piscataway (2020)