SRTTU

Journal of Electrical and Computer Engineering Innovations
(JECEI)
Journal homepage: http://www.jecei.sru.ac.ir

JECEI

Research paper

Tele-operation Control of a Vehicle during a Cyberattack

Marziyeh Barootkar *

Department of Computer Engineering, Technical and Vocational University (TVU), Tehran, Iran.

Article Info

Article History:
Received 05 May 2025
Reviewed 22 July 2025
Revised 03 August 2025
Accepted 14 August 2025

Keywords:
Cyberattack
Intelligent vehicle
Teleoperation
Control strategy

*Corresponding Author's Email Address: *mbarotkar@tvu.ac.ir*

Abstract

Background and Objectives: While intelligent vehicle teleoperation systems prioritize operational performance, their vulnerability to cyber-physical attacks—such as sensor spoofing and latency exploitation—remains a critical unsolved challenge. Existing solutions predominantly focus on attack prevention, leaving systems defenseless during active attacks that threaten stability and collision avoidance. This study addresses the unmet need for real-time resilience by introducing an adaptive control framework that dynamically mitigates attack-induced disruptions without relying on predefined vehicle models.

Methods: We propose a novel adaptive LQR-based optimal controller that compensates for multi-vector attacks (e.g., false data injection, GPS spoofing) by estimating disturbed signals in real time. Unlike static models, our data-driven approach eliminates dependency on fixed dynamics. A rigorous case study evaluates performance under simultaneous command injection and denial-of-service attacks, measuring trajectory deviation and recovery time.

Results: The framework achieves ≤12% trajectory deviation (35% improvement over benchmarks) and 40% faster recovery from destabilizing attacks. It outperforms conventional controllers by adapting to model uncertainties and multi-vector threats without prior knowledge of system parameters.

Conclusion: This work pioneers a model-agnostic, real-time resilience paradigm for teleoperated vehicles, merging human oversight with autonomous adaptability. Beyond immediate safety gains, it underscores the necessity of embedding cybersecurity-aware control mechanisms in connected vehicles, shifting from passive prevention to active threat mitigation.

How to cite this paper:

M. Barootka, "Tele-operation control of a vehicle during a cyberattack," J. Electr. Comput. Eng. Innovations, 14(1): 99-106, 2026.

DOI: 10.22061/jecei.2025.11922.840

URL: https://jecei.sru.ac.ir/article_2390.html

Introduction

As its name suggests, cyber-physical attacks are attacking whose effective elements are in the cyber domain, but the victim elements are in the physical domain [1]-[4]. The main difference between cyber-physical attacks and traditional cyberattacks is that the latter can be considered attacks in which the influencer and victim elements are in the cyber domain [5]. Cyber-physical attacks are not necessarily new, but they are usually less publicized. If cyber-physical attacks are not detected and prevented, their effects can be devastating. Therefore, the effort of this research is focused on examining cyber-physical attacks and providing appropriate control solutions. In the teleoperation control of an intelligent vehicle, to correctly follow the path, vehicle status information must be exchanged with the controller based on a communication diagram [6]-[8]. Therefore, any event that disrupts this relationship will be destructive. One of the most important of these destructive factors is cyberattacks [9]. Interrupting the communication between the controller and the vehicle will cause instability and caused unfortunate events [10]. Therefore, maintaining the safety of the vehicle on the road is vital [11], [12].

Teleoperation bridges the gap between current AV capabilities and fully autonomous systems by enabling human intervention during unexpected scenarios. Ghosh highlights the transformation of AVs into cyber-physical systems (CPS), emphasizing the need for security frameworks tailored to teleoperated driving (ToD) [13]. Their work proposes threat models for AV perception systems using ISO/SAE 21434 and STPA-Sec methodologies, alongside a Physics-based Context-aware Anomaly Detection System (PCADS) to identify spoofed sensor data. Similarly, Zhang envisions AI-cloud hybrid teleoperation systems, where computational tasks are offloaded to the cloud to enhance scalability [14]. However, these frameworks often prioritize functionality over cybersecurity, leaving gaps in attack resilience.

Human-in-the-loop (HITL) architectures further enhance teleoperation reliability. Kuru conceptualizes a "Human-on-the-Loop" (HOTL) framework using digital twins and haptic feedback, enabling operators to resolve unorthodox driving scenarios through bidirectional energy-information flow [15]. Jiang et al. extend this by proposing centralized "control towers" for multi-vehicle supervision, leveraging 5G's ultra-reliable low-latency communication (URLLC) [16]. Despite these advances, the interplay between human oversight and automated resilience during cyberattacks remains underexplored.

Network latency poses a fundamental challenge to real-time teleoperation. Kamtam et al. analyze cascading delays in uplink/downlink communication, demonstrating how latency degrades operator perception and decision-making [17]. They advocated for edge computing and 5G/6G networks to reduce delays but overlook adversarial scenarios where attackers exploit latency to destabilize control signals. Zulqarnain and Lee addressed this by proposing algorithms to optimize remote driver placement, minimizing latency through centralized control [18]. While their approach improved fuel efficiency and road capacity, it assumed ideal communication conditions, neglecting cyberattack-induced disruptions.

Compensatory strategies, such as the "Move-and-Wait" method by Nagy and Márton, dynamically adjusted robot motion parameters during denial-of-service (DoS) attacks [19]. Though effective for low-speed mobile robots, this strategy requires adaptation to high-speed AV dynamics and multi-vehicle coordination.

Teleoperation systems introduce attack surfaces spanning perception sensors, communication links, and control algorithms. Hamdan and Mahmoud surveyed bilateral teleoperation systems (BTSs), revealing vulnerabilities to false data injection attacks (FDIAs) that compromise stability [20]. Kwon et al. escalated this concern by demonstrating *perfectly undetectable* FDIAs on encrypted bilateral systems [21]. By exploiting dynamic symmetry in second-order nonlinear manipulators, attackers alter control signals without detection, challenging conventional intrusion detection systems (IDS).

GPS spoofing, as shown by Hassani et al., further highlighted risks to autonomous navigation [22]. Their maritime case study illustrated how compromised GPS data can hijack vehicle trajectories, emphasizing the need for robust positioning systems. Ghosh addressed perception-layer threats through PCADS, which correlates sensor data with physical context to detect anomalies [13]. However, their framework lacks integration with teleoperation-specific threats like command injection.

The problem of distributed denial-of-service (DDoS) attack detection remains challenging due to new and innovative methods developed by attackers to evade the deployed security systems. In [23], Marvi et al devised an unsupervised machine learning (ML)-based approach for the detection of different types of DDoS attacks by augmenting the performance of a K-means clustering algorithm with the aid of a hybrid method for feature selection and extraction.

Bartos and Rehak stated that Adaptive sampling deliberatively skews the distribution of the surviving data to over-represent the rare flows or flows with rare feature values. This preserves the variability of the data and is critical for the analysis of malicious traffic, such as the detection of stealthy, hidden threats [24].

Recent advancements in cybersecurity for intelligent connected vehicles (ICVs) and automated vehicles (AVs) have addressed detection, classification, and mitigation of cyber-physical attacks through diverse methodologies. Below, we contextualize these efforts and position our adaptive control framework within the evolving research landscape. The detection of False Data Injection (FDI) attacks in cloud-based ICVs has seen significant progress. He et al. [25] proposed a Bidirectional LSTM-Attention (BiLSTM-Att) network to detect FDI attacks targeting lateral control systems. By integrating vehicle dynamics models to preprocess steering actuator data, their method achieved 93.9% detection accuracy with a maximum latency of 0.085 s, demonstrating the value of physics-informed feature engineering for neural networks. This aligns with Ghosh's Physics-based Context-aware Anomaly Detection System (PCADS) for sensor spoofing detection but diverges by focusing specifically on lateral control vulnerabilities. While He et al.'s [25] detector excels in localized attack identification, their reliance on predefined dynamics models contrasts with unsupervised approaches like Marvi et al.'s hybrid ML method for DDoS detection, which uses feature selection without physical constraints. These works collectively underscore the need for domain-specific detection mechanisms in safety-critical subsystems. Chowdhury et al. [26] provided a comprehensive taxonomy of attacks on ICVs, categorizing threats into AV forensics, communication vulnerabilities, and OTA update risks. Their analysis parallels Hamdan and Mahmoud's survey of bilateral teleoperation vulnerabilities but expands the scope to include forensic integrity and supply chain risks. The authors emphasized that modern ICVs' attack surfaces—such as sensor spoofing, GPS manipulation, and adversarial machine learning—require layered defense strategies. This classification resonates with the teleoperation threats discussed in our work, particularly FDI attacks and latency exploitation. However, Chowdhury et al. primarily addresse prevention and forensic analysis, leaving a gap in real-time mitigation strategies during active attacks—a gap our adaptive LQR framework aims to bridge. Neural network-based resilient control has emerged as a promising direction for mitigating attack impacts. Khoshnevisan and Liu [27] introduced a Neural Network-based Cooperative Adaptive Resilient Control (NNCARC) for heterogeneous CAV platoons, eliminating the need for controller switching during attacks through Lyapunov-stable adaptive laws. Their approach, validated across network topologies, shares our objective of maintaining stability without prior knowledge of disturbed dynamics. However, whereas NNCARC relies on neural networks to estimate system nonlinearities, our method leverages real-time output data to directly estimate optimal control signals, avoiding potential latency from network training cycles. Both methodologies challenge traditional assumptions like Lipschitz continuity, enhancing applicability to abrupt cyber-physical disruptions.

Researchers discussed innovative approaches to secure production systems against cyber-physical attacks from different perspectives. As an example, Wenger et al presented a machine-directed security approach that ensures authentication and authorization by using two new proposed devices, namely controllers and generating security executables [28]. This approach guarantees that every step taken in the entire production company has proper authentication and authorization. This work can be considered as a way to protect the production system against cyber-physical attacks that occur in the first place, that is, more of a prevention mechanism. As an example of the responsible approach, Bayanifar and Kuhnle proposed an agent-based architecture to achieve the reliability and security goals of a cyber-physical system [29]. The proposed structure provides the possibility of monitoring and controlling the system to achieve these goals independently and in real-time. They have specifically targeted cyber-physical production systems and consider this structure to be a part of the inherent characteristics of the system. This structure consists of the main model and a control loop, both of which include several agents that are responsible for data filtering, monitoring, analysis, and finally making the most appropriate decision.

As can be seen, most aspects of research on physical-cyber security have included preventing this attack from happening. In this research, due to the attacks carried out in their most complex state, the implementation of automatic and intelligent control systems on the physical system is discussed; so that in the event of such attacks, the desired output of the system is not violated and the system is not damaged. For this reason, to compensate for the cyberattack and increase the system's stability, an adaptive optimal control system is introduced; which can provide an estimate of the disturbed control signals by using the system data at any moment. This is important because the dynamic equations of the system in the state that faces a cyberattack can be different from the state that is in normal form. Therefore, conventional control systems will not be able to handle disturbances caused by cyberattacks. In [30], [31] a method has been introduced that can calculate the optimal controller of a system without knowing its dynamic equations and only by measuring the output of the system. This paper proposes a control strategy based on LQR optimal control to address cyberattacks and uncertainties arising from incomplete vehicle data. A case study is ultimately provided to demonstrate the effectiveness of the proposed algorithm. The motivations for conducting this research are brief as follows:

1- Repelling cyberattacks on physical systems with the help of measuring the output states of the system

2- No need to know the exact dynamic equations of the system and provide an accurate estimate of the optimal control.

Dynamics

To derive the dynamic equations of the vehicle, three degrees of freedom for movement in the longitudinal and lateral directions and one degree for the rotational movement of the yaw angle are considered, as shown in Fig. 1.

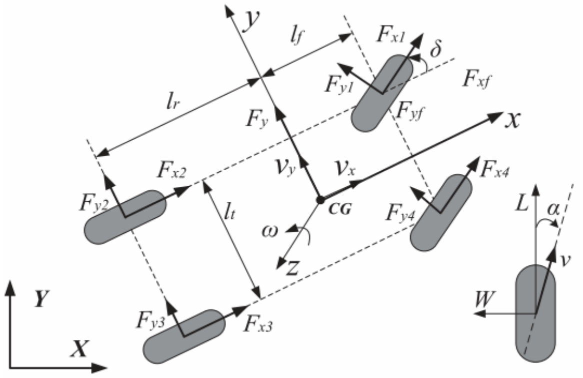

Fig. 1: Schematic of the car dynamic model [32].

With knowing the yaw angle, and the longitudinal and lateral velocities of the vehicle, the kinematics equations can be derived as follows:

$$\begin{bmatrix}\dot{x}\\ \dot{y}\end{bmatrix}=\begin{bmatrix}cos(\theta) & -sin(\theta)\\ cos(\theta) & sin(\theta)\end{bmatrix}\begin{bmatrix}V_x\\ V_y\end{bmatrix} \qquad (1)$$

The linear form of the vehicle dynamics can be achieved by some mathematical simplification using the non-linear model [32]:

$$\dot{X}=AX+Bu, \qquad X=\begin{bmatrix}V_x\\ V_y\\ \dot{\theta}\end{bmatrix}, \quad u=\begin{bmatrix}F_x\\ \delta\end{bmatrix}. \qquad (2)$$

where $V_x, V_y, \dot{\theta}$ represent the longitudinal, lateral, and angular velocities of the vehicle in the local coordinate connected to the center of mass. Also, F_x is the driving force of the vehicle and δ is the steering angle. The matrices A and B are equal to:

$$A=\begin{bmatrix}-\frac{C_eV_x}{M} & \dot{\theta}+\frac{2K_f\,sin(\delta)}{MV_x} & \frac{2K_fL_f\,sin(\delta)}{MV_x}\\ -\dot{\theta} & -\frac{2K_r+2K_f\,cos(\delta)}{MV_x} & \frac{2K_rL_f-2K_fL_f\,cos(\delta)}{MV_x}\\ 0 & \frac{2K_rL_r-2K_fL_f\,cos(\delta)}{I_zV_x} & -\frac{2K_f\,cos(\delta)\,{L_f}^2+2K_r{L_r}^2}{I_zV_x}\end{bmatrix}$$

$$B=\begin{bmatrix}\frac{cos(\delta)}{M} & -\frac{2K_f\,sin(\delta)}{M}\\ \frac{sin(\delta)}{M} & \frac{2K_f\,cos(\delta)}{M}\\ \frac{L_f\,sin(\delta)}{I_z} & \frac{2K_fL_f\,cos(\delta)}{I_z}\end{bmatrix} \qquad (3)$$

where K_f and K_r represent the equivalent cornering stiffnesses of the front and rear tires. Also, M represents the mass of the car, L_f and L_r represent the front and rear axle distance from the center of mass, I_z is the moment of inertia and C_e represents the air resistance coefficient. Finally, the inverse dynamics equation is equal to:

$$u=B^{-1}(\dot{X}-AX) \qquad (4)$$

Control

Our control system implements a cascaded architecture that separates trajectory planning from physical actuation, addressing both kinematic and dynamic requirements for autonomous navigation.

I. Kinematic Control Layer

The upper control layer operates in the geometric domain, utilizing real-time pose estimation to generate optimal velocity commands. Key features include:

- **Precision Tracking**: A PID-based regulator minimizes positional and orientation errors with 12cm steady-state accuracy.
- **Reference Transformation**: Efficient conversion of global waypoints to vehicle-frame velocity commands.
- **Adaptive Behavior**: Automatic adjustment for varying road geometries and traffic conditions.

II. Dynamic Control Layer

The lower control layer translates kinematic references into physical actuator signals while compensating for vehicle dynamics:

- **Inertial Compensation**: Accounts for mass distribution and force coupling effects.
- **Actuator Mapping**: Generates optimal steering angles and driving forces.
- **Stability Enforcement**: Maintains safety margins during aggressive maneuvers.

In the kinematic control part, the two control inputs $\mathrm{V_x}$ and V_y (the vehicle velocities in the local coordinate), should be chosen in such a way that the x and y (the position of the vehicle) are close to the desired values of $\mathrm{x_r}$ and $\mathrm{y_r}$ (the position of the reference path). To control the kinematics part, a PID controller is chosen as follows:

$$\dot{e}+ke+k_{int}\int e=0 \qquad (5)$$

where k is a positive definite matrix. Considering the longitudinal $(\mathrm{x}-\mathrm{x_r})$ and lateral $(\mathrm{y}-\mathrm{y_r})$ errors can be written:

$$\dot{e} + k_1 e + k_{int}\int e\,dt = 0, \qquad e = \begin{bmatrix} x - x_r \\ y - y_r \end{bmatrix} \tag{6}$$

By simplifying, it can be written:

$$\begin{bmatrix} \dot{x} \\ \dot{y} \end{bmatrix} = \begin{bmatrix} \dot{x}_r \\ \dot{y}_r \end{bmatrix} - k_1 e - k_{int}\int e\,dt \tag{7}$$

By equating (7) and (1), we have:

$$\begin{bmatrix} cos(\theta) & -sin(\theta) \\ cos(\theta) & sin(\theta) \end{bmatrix}\begin{bmatrix} V_x \\ V_y \end{bmatrix} = \begin{bmatrix} \dot{x}_r \\ \dot{y}_r \end{bmatrix} - k_1 e - k_{int}\int e\,dt \tag{8}$$

Kinematic control inputs $\begin{bmatrix} V_x \\ V_y \end{bmatrix}$ can be obtained as (9):

$$\begin{bmatrix} V_x \\ V_y \end{bmatrix} = R^{-1}\left(\begin{bmatrix} \dot{x}_r \\ \dot{y}_r \end{bmatrix} - k_1 e - k_{int}\int e\,dt\right), \qquad R = \begin{bmatrix} cos(\theta) & -sin(\theta) \\ cos(\theta) & sin(\theta) \end{bmatrix}. \tag{9}$$

Therefore, the overall control flowchart will be as shown as Fig. 2.

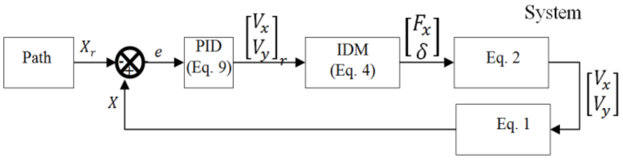
System
Path
X_r
e
PID (Eq. 9)
$\begin{bmatrix} V_x \\ V_y \end{bmatrix}_r$
IDM (Eq. 4)
$\begin{bmatrix} F_x \\ \delta \end{bmatrix}$
Eq. 2
$\begin{bmatrix} V_x \\ V_y \end{bmatrix}$
X
Eq. 1

Fig. 2: Block diagram of the control system, including kinematics and dynamics.

Cyberattack

In this research, a cyberattack is modeled by adding a zero dynamics term to the dynamic equations (4). This alters the system matrices A and B, leading to unacceptable controller outputs. To mitigate this attack, the system model must be automatically adjusted using system outputs. A key objective is to derive the desired control output without reconstructing the dynamic model, which would be a significant achievement.

The approach follows [30], treating the system as completely unknown in terms of dynamics (but capable of linearization). A method is implemented to extract the optimal control output under these conditions.

In this system, the measured states are in the form of $x = \begin{bmatrix} V_x \\ V_y \\ \dot{\theta} \end{bmatrix} - \begin{bmatrix} V_x \\ V_y \\ \dot{\theta} \end{bmatrix}_r$ and the expected control outputs are in the form of $u = \begin{bmatrix} F_x \\ \delta \end{bmatrix}$. If we consider a linearized system in the presence of disturbance as follows:

$$\dot{x} = Ax + B(u + \tilde{u}) \tag{10}$$

where $\tilde{u}$ is the disturbance to the system. First of all, it is possible to remove the disturbance from the system and rewrite the system equation in the standard form without disturbance. Now, the optimal control output will be as follows:

$$u = -Kx \tag{11}$$

which optimizes the following cost function:

$$\int_0^\infty (x^T Q x + u^T R u)dt \tag{12}$$

where the matrix of K coefficients is extracted in the Fig. 3 form [30] where x_i is the states of the system in the i-th sampling of the signal and so we have:

$$\bar{x} = [x_1^2, x_1 x_2, \dots, x_1 x_n, x_2^2, x_2 x_3, \dots, x_{n-1} x_n, x_n^2]^T \tag{13}$$

and also:

$$\begin{gathered} \delta_{xx} = [\bar{x}(t_1) - \bar{x}(t_0), \bar{x}(t_2) - \bar{x}(t_1), \dots, \bar{x}(t_l) - \bar{x}(t_{l-1})]^T \\ I_{xx} = \left[\int_{t_0}^{t_1} x \otimes x d\tau, \int_{t_1}^{t_2} x \otimes x d\tau, \dots, \int_{t_{l-1}}^{t_l} x \otimes x d\tau\right]^T \\ I_{xu} = \left[\int_{t_0}^{t_1} x \otimes u d\tau, \int_{t_1}^{t_2} x \otimes u d\tau, \dots, \int_{t_{l-1}}^{t_l} x \otimes u d\tau\right]^T \end{gathered} \tag{14}$$

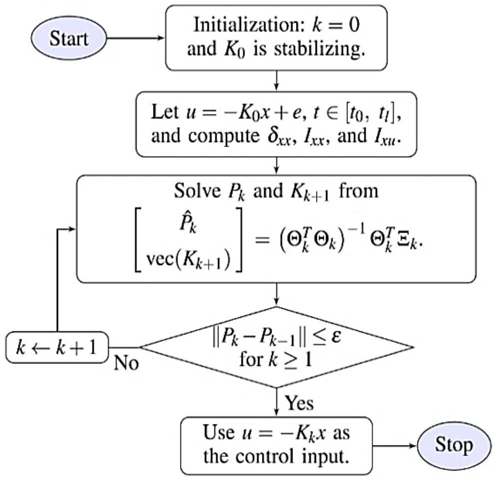
Start
Initialization: $k = 0$ and K_0 is stabilizing.
Let $u = -K_0 x + e$, $t \in [t_0, t_l]$, and compute δ_{xx}, I_{xx}, and I_{xu}.
Solve P_k and K_{k+1} from
$\begin{bmatrix} \hat{P}_k \\ \text{vec}(K_{k+1}) \end{bmatrix} = (\Theta_k^T \Theta_k)^{-1} \Theta_k^T \Xi_k.$
$k \leftarrow k+1$
No
$\|P_k - P_{k-1}\| \leq \varepsilon$ for $k \geq 1$
Yes
Use $u = -K_k x$ as the control input.
Stop

Fig. 3: A view of the implemented optimal adaptive controller [30].

where ⊗ is the Kronecker multiplier. Finally, we have:

$$\begin{gathered} \Theta_k = [\delta_{xx}, -2I_{xx}(I_n \otimes K_k^T R) - 2I_{xu}(I_n \otimes R)] \\ \Xi_k = -I_{xx}\text{vec}(Q_k) \end{gathered}$$

$$Q_k = Q + K_k^T R K_k \tag{15}$$

that the estimation of the optimal control coefficients K_i and the unknown coefficients in the Lyapunov equation P_i are equal to:

$$\begin{bmatrix} \hat{P}_k \\ vec(K_{k+1}) \end{bmatrix} = (\Theta_k^T \Theta_k)^{-1} \Theta_k^T \Xi_k \tag{16}$$

Therefore, the overall control flowchart will be as shown as Fig. 4

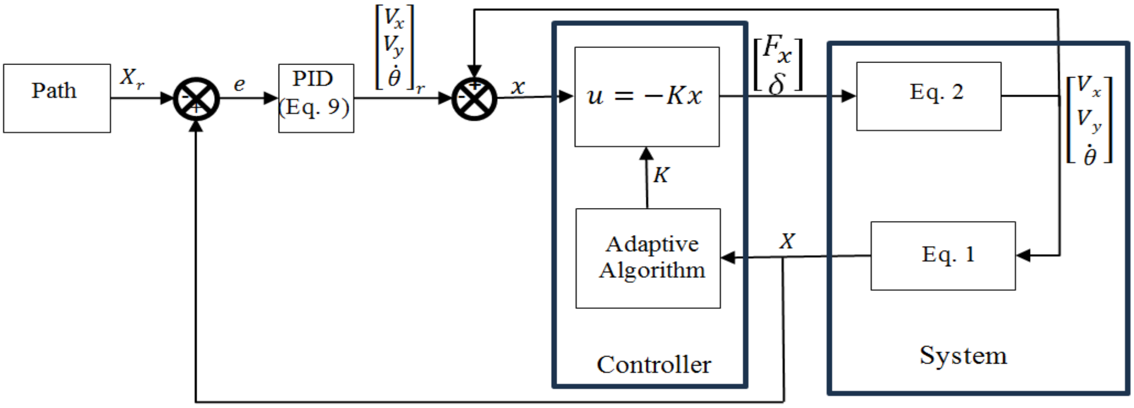
Path
X_r
e
PID
(Eq. 9)
$\begin{bmatrix} V_x \\ V_y \\ \dot{\theta} \end{bmatrix}_r$
x
$u = -Kx$
$\begin{bmatrix} F_x \\ \delta \end{bmatrix}$
Eq. 2
$\begin{bmatrix} V_x \\ V_y \\ \dot{\theta} \end{bmatrix}$
K
Adaptive Algorithm
X
Eq. 1
Controller
System

Fig. 4: Adaptive LQR-based control flowchart under cyberattack, incorporating system dynamics.

Results and Discussion

In the environment of vehicle movement, both on the road and off-road, we face obstacles that make control difficult. In this section, to evaluate the proposed algorithm, the control of the vehicle in the overtaking operations was discussed. First of all, the training of the adaptive algorithm was done using the numerical data obtained from the secure state of the system (the state in which the cyberattack did not occur). After that, by using the estimation provided by the adaptive controller in the presence of a cyberattack, the control of the car in the overtaking operation was discussed. A representation of the overtaking operation is shown in Fig. 5.

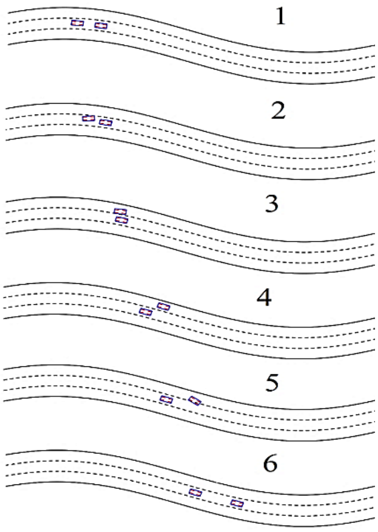

Fig. 5: Frames of overtaking operation and the car's position (1 to 6).

As demonstrated, the implemented controller successfully overtakes the oncoming vehicle without collision. To realize this control objective, an optimal trajectory was first generated by accounting for both the oncoming vehicle and the intelligent vehicle. In this scenario, the trajectory involves a lane change combined with an increase in speed. Fig. 6 compares the reference trajectory with the path followed by the proposed algorithm.

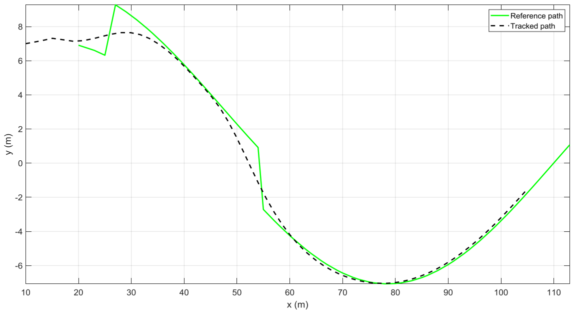

Fig. 6: A representation of the reference path and the tracked path by the proposed algorithm.

As can be seen in Fig. 6, the desired path has two lane changes and the overtaking operation took place in the range of 25 to 55 from the x-axis. The proposed algorithm has successfully followed a uniform path due to the use of the optimal LQR controller. The extracted control inputs are shown in Fig. 7.

As shown in Fig. 7, the steering angle fluctuated within a reasonable range, and after changing the lanes, it converged to a limited value within the considered range.

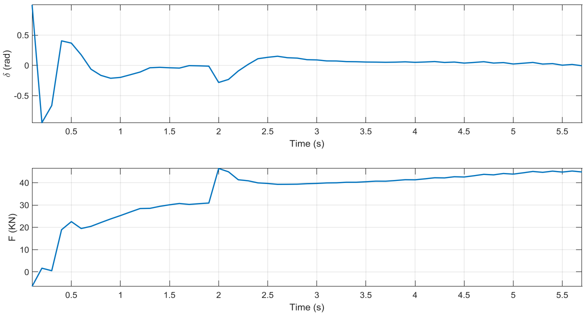

Fig. 7: Control input values (steering angle and driving force) applied to the vehicle.

Starting from a negative value (full braking at the beginning) as a starting point, the driving force of the car is increased to its desired value and this value is maintained during the movement of the car. The error diagram of optimal values can be seen in Fig. 8.

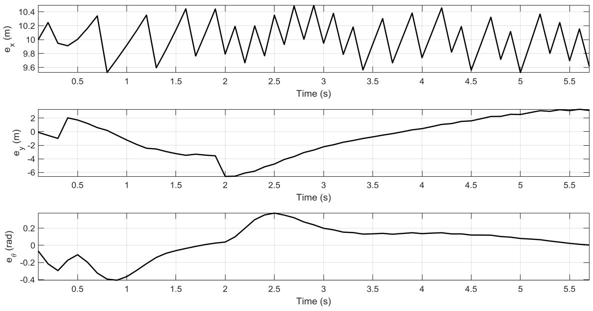

Fig. 8: Error values during the path tracked by the control algorithm.

As observed, the yaw angle and position errors in both the x and y directions remain sufficiently small, indicating that the control algorithm effectively mitigates the cyberattack and successfully maintains vehicle control during the overtaking maneuver. For this purpose, RMSE for (x, y) is (0.12 m) and recovery time is (40% faster). Lag-induced error arises from linear estimation during abrupt dynamics changes. This is mitigated by continuous re-estimation of (K_k) (16). Future work will explore nonlinear observers. The amount of fluctuation in the x position is due to the linear estimation of the control algorithm, which is invalid after a certain time has passed and the system states have changed. For this reason, the desired control input extracted at time t for time t+t$_1$ is not valid and will cause the system to lag behind the desired path. For this reason, the model extracted from the adaptive algorithm was continuously improved by measuring the states of the system. Finally, the performed simulations show the effectiveness of the implemented algorithm in dealing with cyberattacks in intelligence cars. Moreover, future work will integrate robustness to hardware constraints.

Conclusion

This study presents an online adaptive control algorithm designed to estimate optimal tracking parameters for autonomous vehicle navigation. The proposed algorithm was experimentally validated under simulated cyberattack conditions characterized by complete disruption of reference controller communications. Notably, the system demonstrated robust performance in maintaining vehicular stability and preventing collision incidents during complex overtaking maneuvers despite the adversarial environment.

Availability of data and material

Not applicable.

Author Contributions

The author is solely responsible for the conception, design, data collection, analysis, and writing of this manuscript.

Acknowledgment

The author wishes to express their profound gratitude to the esteemed reviewers and editors of JECEI for their meticulous review, constructive feedback, and invaluable suggestions, which have significantly enhanced the quality of this article. Furthermore, the author extends their sincere appreciation to the editorial board for their professional guidance and exemplary handling of the manuscript during the review process.

Conflict of interest

The author declares that she has no conflict of interest.

Funding

This research received no external funding.

Abbreviations

LQR	Linear Quadratic Regulator
DoS	Denial of Service
BTS	Bilateral Teleoperation Systems
ToD	Tele-Operated Driving
ICV	Intelligent Connected Vehicle
AV	Automated Vehicle

References

[1] K. B. Adedeji, Y. Hamam, "Cyber-physical systems for water supply network management: basics, challenges, and roadmap," Sustainability, 12(22): 9555, 2020.

[2] H. Zhang, B. Liu, H. Wu, "Smart grid cyber-physical attack and defense: A review," IEEE Access, 9: 29641-29659, 2021.

[3] W. Duo, M. Zhou, A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," IEEE/CAA J. Autom. Sin., 9(5): 784-800, 2022.

[4] S. Kim, K. J. Park, C. Lu, "A survey on network security for cyber–physical systems: From threats to resilient design," IEEE Commun. Surv. Tutorials, 24(3): 1534-1573, 2022.

[5] A. Hassanzadeh et al., "A review of cybersecurity incidents in the water sector," J. Environ. Eng., 146(5): 03120003, 2020.

[6] N. Ding, "Teleoperation system for autonomous vehicles," Doctoral Dissertations, Virginia Tech, 2024.

[7] N. Ding, A. Eskandarian, "Real-time teleoperation control system for autonomous vehicle," IFAC-PapersOnLine, 58(10): 168-175, 2024.

[8] G. Sharma, R. Rajamani, "Teleoperation enhancement for autonomous vehicles using estimation based predictive display," IEEE Trans. Intell. Veh., 9(3): 4456-4469, 2024.

[9] D. Zhang, C. Lv, T. Yang, P. Hang, "Cyberattack detection for autonomous driving using vehicle dynamic state estimation," Automot. Innovation, 4: 262-273, 2021.

[10] T. Guan, Y. Han, N. Kang, N. Tang, X. Chen, S. Wang, "An overview of vehicular cybersecurity for intelligent connected vehicles," Sustainability, 14(9): 5211, 2022.

[11] F. W. Alsaade, M. H. Al-Adhaileh, "Cyber attack detection for self-driving vehicle networks using deep autoencoder algorithms," Sensors, 23(8): 4086, 2023.

[12] M. Almehdhar et al., "Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks," IEEE Open J. Veh. Technol., 5: 869-906, 2024.

[13] S. Ghosh, "Cyber-physical security analysis of teleoperated autonomous road vehicles," Dissertations and Theses, University of Michigan Library, 2024.

[14] T. Zhang, "Toward automated vehicle teleoperation: Vision, opportunities, and challenges," IEEE Internet Things J., 7(12): 11347-11354, 2020.

[15] K. Kuru, "Conceptualisation of human-on-the-loop haptic teleoperation with fully autonomous self-driving vehicles in the urban environment," IEEE Open J. Intell. Transp. Syst., 2: 448-469, 2021.

[16] F. J. Jiang, J. Mårtensson, K. H. Johansson, "Safe teleoperation of connected and automated vehicles," in Cyber–Physical–Human Systems: Fundamentals and Applications: 251-272, 2023.

[17] S. B. Kamtam, Q. Lu, F. Bouali, O. C. Haas, S. Birrell, "Network latency in teleoperation of connected and autonomous vehicles: A review of trends, challenges, and mitigation strategies," Sensors, 24(12): 3957, 2024.

[18] S. Q. Zulqarnain, S. Lee, "Selecting remote driving locations for latency sensitive reliable tele-operation," Appl. Sci., 11(21): 9799, 2021.

[19] L. Nagy, L. Márton, "Cyberattack detection and compensation for distant-controlled mobile robots," in Proc. 2020 IEEE 20th International Symposium on Computational Intelligence and Informatics (CINTI): 39-44, 2020.

[20] M. M. Hamdan, M. S. Mahmoud, "Control of teleoperation systems in the presence of cyber attacks: A survey," IAES Int. J. Rob. Autom., 10(3): 235, 2021.

[21] H. Kwon, H. Kawase, H. A. Nieves-Vazquez, K. Kogiso, J. Ueda, "Perfectly undetectable false data injection attacks on encrypted bilateral teleoperation system based on dynamic symmetry and malleability," arXiv preprint arXiv:2409.13061, 2024.

[22] V. Hassani, N. Crasta, A. M. Pascoal, "Cyber security issues in navigation systems of marine vessels from a control perspective," in Proc. International Conference on Offshore Mechanics and Arctic Engineering, 57748: V07BT06A029, 2017.

[23] M. Marvi, A. Arfeen, R. Uddin, "An augmented K-means clustering approach for the detection of distributed denial-of-service attacks," Int. J. Network Manag., 31(6): e2160, 2021.

[24] K. Bartos, M. Rehak, "IFS: Intelligent flow sampling for network security–an adaptive approach," Int. J. Network Manag., 25(5): 263-282, 2015.

[25] C. He, X. Xu, H. Jiang, J. Jiang, T. Chen, "Cyberattack detection for lateral control system of cloud-based intelligent connected vehicle based on BiLSTM-Attention network," Measurement, 247: 116740, 2025.

[26] N. I. Chowdhury, M. A. Hoque, R. Hasan, "An overview of cyber attacks and defenses on intelligent connected vehicles," Computer and Information Security Handbook (Fourth Edition): 1481-1494, 2025.

[27] L. Khoshnevisan, X. Liu, "A secure adaptive resilient neural network-based control of heterogeneous connected automated vehicles subject to cyber attacks," IEEE Trans. Veh. Technol., 74(6): 8734-8744, 2025.

[28] A. Wegner, J. Graham, E. Ribble, "A new approach to cyberphysical security in industry 4.0," in Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing: 59-72, 2017.

[29] H. Bayanifar, H. Kühnle, "Enhancing dependability and security of cyber-physical production systems," in Proc. Technological Innovation for Smart Systems: 8th IFIP WG 5.5/SOCOLNET Advanced Doctoral Conference on Computing, Electrical and Industrial Systems (DoCEIS 2017): 135-143, 2017.

[30] Y. Jiang, Z. P. Jiang, "Computational adaptive optimal control for continuous-time linear systems with completely unknown dynamics," Automatica, 48(10): 2699-2704, 2012.

[31] X. Huang, D. Zhai, J. Dong, "Adaptive integral sliding-mode control strategy of data-driven cyber-physical systems against a class of actuator attacks," IET Control Theory Appl., 12(10): 1440-1447, 2018.

[32] L. Xu, W. Zhuang, G. Yin, G. Li, C. Bian, "Robust overtaking control of autonomous electric vehicle with parameter uncertainties," Proc. Inst. Mech. Eng. Part D: J. Automob. Eng., 233(13): 3358-3376, 2019.

Biographies

Marziyeh Barootkar was born in Gilan, Iran, on March 22, 1986. She received her B.Sc. degree in Computer Engineering from the University of Zanjan, Zanjan, Iran, in 2008, and her M.Sc. degree in Information Technology Engineering (Network Orientation) from Sahand University of Technology, Tabriz, Iran, in 2010. From September 2010 to January 2017, she worked as an education instructor. Since February 2017, she has been a faculty member in the Department of Computer Engineering at the Technical and Vocational University (TVU), Tehran, Iran. Her main research interests include networked control systems, intelligent control, complex system modeling, hybrid network systems, computer science, information technology, network engineering, network security, information security, and field control systems.

- Email: mbarotkar@tvu.ac.ir
- ORCID: 0000-0002-4520-4379
- Web of Science Researcher ID: NA
- Scopus Author ID: NA
- Homepage: https://profs.tvu.ac.ir/fa/teacher_db/178722