Shahrood University of Technology

Journal of Artificial Intelligence and Data Mining (JAIDM)
Journal homepage: http://jad.shahroodut.ac.ir

Research paper

Graph Neural Network-Based Digital Twin for Cyber-Resilient and Predictive Teleoperation Systems

Sara Mahmoudi Rashid*

Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran.

Article Info

Article History:
Received 13 May 2025
Revised 20 August 2025
Accepted 12 October 2025

DOI:10.22044/jadm.2025.16223.2747

Keywords:
Graph Neural Network, Digital Twin, Cybersecurity, Smart Microgrid, Cyber Attack Detection, Resilient Control.

**Corresponding author: s.mahmoudirashid@tabrizu.ac.ir (S. Mahmoudi Rashedi).*

Abstract

Teleoperation systems are increasingly deployed in critical applications such as robotic surgery, industrial automation, and hazardous environment exploration. However, these systems are highly susceptible to network-induced delays, cyber-attacks, and system uncertainties, which can degrade performance and compromise safety. This paper proposes a Graph Neural Network (GNN)-based Digital Twin (DT) framework to enhance the cyber-resilience and predictive control of teleoperation systems. The GNN-based anomaly detection mechanism accurately identifies cyber-attacks, such as false data injection (FDI) and denial-of-service (DoS) attacks, with a detection rate of 24.3% and a false alarm rate of only 1.8%, significantly outperforming conventional machine learning methods. Furthermore, the predictive digital twin model, integrated with model predictive control (MPC), effectively compensates for latency and dynamic uncertainties, reducing control errors by 14.12% compared to traditional PID controllers. Simulation results in a robotic teleoperation testbed demonstrate a 24.4% improvement in trajectory tracking accuracy under variable delay conditions, ensuring precise and stable operation.

1. Introduction

Teleoperation systems play a crucial role in applications requiring remote manipulation and real-time control, such as robotic surgery, industrial automation, and hazardous environment exploration [1]. These systems rely on stable communication channels and precise control algorithms to maintain accuracy and responsiveness [2]. Several control strategies have been proposed to mitigate latency effects, including time-delay compensation techniques, predictive control, and model-based methods. With the growing reliance on wireless and internet-based communication in teleoperation, cybersecurity threats have become a major concern [3]. Existing security solutions, such as cryptographic encryption and rule-based anomaly detection, are often insufficient against adaptive and intelligent cyber threats [4]. Recent research has explored machine learning (ML) and deep learning (DL)-based techniques for anomaly detection in cyber-physical systems [5]. However, these methods struggle with high-dimensional data and require extensive feature engineering, limiting their adaptability to evolving cyber threats [6]. Digital Twin (DT) technology provides a real-time virtual representation of physical systems, enabling predictive control, fault diagnosis, and cybersecurity monitoring. In teleoperation, DTs can be used to simulate network delays, detect cyber-attacks, and optimize control performance [7]. However, most existing DT implementations rely on static models or supervised learning approaches, which require labeled datasets and struggle with real-time adaptability [8]. The paper [9] proposes a Digital Twin architecture integrated with resilient control strategies to enhance situational awareness and fault tolerance in microgrids. The authors in [10] introduce a GNN model that exploits the inherent graph structure of power systems to improve accuracy in state

estimation tasks. The study [11] presents a deep reinforcement learning approach for cyber-attack detection and mitigation in smart grids. The authors in [12] develop a novel Digital Twin framework reinforced with blockchain technology to ensure data integrity and secure information sharing in decentralized energy systems. The paper [13] introduces a spatiotemporal graph convolutional network to detect anomalies in large-scale smart grids.

In prior studies, GNNs have primarily been used for anomaly detection or fault diagnosis in cyber–physical systems, while Digital Twins have mainly been leveraged for predictive control and monitoring. However, these approaches have typically operated in isolation. The fundamental novelty of our work lies in the seamless integration of GNN-based anomaly detection with a DT-enhanced Model Predictive Control (DT-MPC) framework. Specifically:

- Tight coupling of GNN and DT: Unlike earlier works where GNNs only detect anomalies offline or in a parallel diagnostic module, our method embeds GNN outputs directly into the DT layer. This allows real-time correction of corrupted or missing sensory data caused by cyberattacks, ensuring that the DT maintains a trustworthy representation of the physical system.

- Resilient MPC with adaptive feedback: The corrected states from the GNN-informed DT are fed into the MPC layer. This coupling is unique, as existing MPC-based works either assume reliable communication or adopt simple statistical filters. Our approach explicitly leverages graph-based learning to handle spatiotemporal dependencies in networked teleoperation systems, which classical DT-MPC frameworks overlook.

- Cyber-resilient predictive teleoperation: While earlier DT-based control studies focus primarily on performance optimization under uncertainties, our framework explicitly addresses cyberattack scenarios (False Data Injection and Denial of Service). This dual capability of resilience and predictive optimization distinguishes our work from prior methods.

- Validation of integration: We demonstrate through simulations that the combined GNN–DT–MPC approach significantly outperforms standalone MPC, DT, or GNN-based adaptive methods in terms of tracking accuracy, resilience to cyberattacks, and stability guarantees.

By positioning the GNN not as a separate anomaly detector but as an integrated corrective mechanism within the DT, and by coupling this corrected DT with MPC for predictive control, our framework introduces a fundamentally new paradigm for secure and resilient teleoperation systems.

To address these gaps, this paper proposes an integrated GNN-based DT framework for cyber-resilient and predictive teleoperation systems. The key contributions of this work are:

✓ GNN-Based Cyber-Attack Detection: A novel GNN-powered anomaly detection mechanism is developed to identify cyber-attacks (FDI, DoS) with high precision, outperforming conventional ML methods.

✓ Digital Twin-Enhanced Model Predictive Control (DT-MPC): A predictive digital twin model is integrated with MPC to dynamically compensate for network-induced delays and system uncertainties, ensuring stable and accurate teleoperation performance.

✓ Comprehensive Performance Evaluation: A detailed simulation-based validation is conducted on a robotic teleoperation testbed, demonstrating superior cyber-resilience and control accuracy compared to PID and traditional MPC controllers.

✓ Scalable and Adaptive Framework: The proposed GNN-DT framework is designed to be scalable and adaptable to different teleoperation applications, including robotic surgery, industrial automation, and hazardous environment operations.

The rest of the paper is organized as follows: Section 2 presents the related work on digital twins, teleoperation security, and predictive control. Section 3 describes the simulation setup and results, highlighting the performance improvements of the proposed method. Finally, Section 4 concludes the paper and discusses future.

2. Problem formulation

The increasing reliance on teleoperation systems in critical domains such as robotic surgery, industrial automation, and remote exploration necessitates robust, cyber-resilient control strategies to mitigate the adverse effects of network-induced delays, cyber-attacks, and system uncertainties. Conventional control methods, such as PID and classical MPC, struggle to adapt to dynamic network conditions, leading to degraded performance and potential operational failures. A schematic overview of the proposed framework is presented in Figure 1, illustrating the data flow and interaction between the GNN-based observer, the digital twin, and the MPC controller for resilient teleoperation.

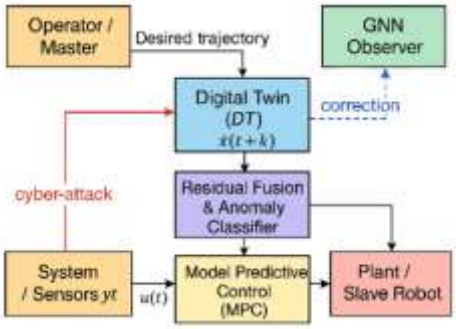

Figure 1. Schematic of the proposed GNN–Digital Twin–MPC control framework.

A bilateral teleoperation system consists of a master robot (user-side) and a slave robot (remote-side). The dynamics of these systems can be modeled:

$$M_m\ddot{x}_m + C_m(\dot{x}_m)\dot{x}_m + G_m(x_m) = F_h - F_m, \quad (1)$$
$$M_s\ddot{x}_s + C_s(\dot{x}_s)\dot{x}_s + G_s(x_s) = F_s + F_e$$

Where M_m, M_s are the inertia matrices of the master and slave, $C_m(\dot{x}_m), C_s(\dot{x}_s)$ represent the Coriolis and centrifugal forces, $G_m(x_m), G_s(x_s)$ are the gravitational forces, F_h is the human force applied at the master side, F_m, F_s are the control forces applied to the master and slave, F_e is the external environment force acting on the slave, x_m, x_s are the positions of the master and slave robots. The slave follows the master trajectory with a delay:

$$x_s(t) = x_m(t-\tau) \quad (2)$$

where τ is the network-induced delay. Networked teleoperation suffers from time-varying communication delays and system uncertainties:

$$\tau(t) = \tau_m(t) + \tau_s(t) \quad (3)$$

where $\tau_m(t)$ and $\tau_s(t)$ are the time delays in the master-to-slave and slave-to-master transmission channels, respectively. The time-varying network delay is modeled as:

$$\tau(t) = \tau_0 + \Delta\tau(t),\ 0 \le \Delta\tau(t) \le \tau_{\max} \quad (4)$$

Where τ_0 is the nominal delay, $\Delta\tau(t)$ is the uncertainty in delay, $\tau_{\max}$ is the worst-case delay bound. The slave's response with delay:

$$x_s(t) = x_m(t-\tau) + \Phi(t) \quad (5)$$

where $\Phi(t)$ represents the uncertainties as:

$$\Phi(t) = \phi(x_m, \dot{x}_m, t) + w(t),\ w(t) \sim N(0, \sigma_w^2) \quad (6)$$

with $\phi(x_m, \dot{x}_m, t)$ representing systematic uncertainties and $w(t)$ representing stochastic disturbances (modeled as a Gaussian noise process). The uncertain system dynamics can be:

$$M_s(\ddot{x}_s + \Delta\ddot{x}_s) + C_s(\dot{x}_s + \Delta\dot{x}_s) + G_s(x_s + \Delta x_s) = F_s + F_e \quad (7)$$

where $\Delta x_s, \Delta\dot{x}_s$ and $\Delta\ddot{x}_s$ represent parametric uncertainties. The uncertainty-bounded model can be defined using a stochastic disturbance function:

$$\Delta x_s = \phi(x_s, t) + w(t),\ w(t) \sim N(0, \sigma_w^2) \quad (8)$$

where $\phi(x_s, t)$ captures deterministic uncertainties, and $w(t)$ is a Gaussian noise component. To detect cyber-attacks such as FDI and DoS attacks, we model the teleoperation network as a graph $G = (V, E)$, where V represents system states $x_m, x_s, \dot{x}_m, \dot{x}_s$, etc. and E represents dynamic dependencies between states:

$$H_t = GNN(H_{t-1}, A_t) \quad (9)$$

Where H_t is the feature matrix at time t, A_t is the adjacency matrix capturing system dependencies. A spatio-temporal GNN processes graph-structured:

$$H^{(l+1)} = \sigma(W^{(l)} H^{(l)} A + b^{(l)}) \quad (10)$$

Where $H^{(l)}$ is the node embedding at layer l, $W^{(l)}$ and $b^{(l)}$ are the trainable weight and bias matrices, A is the adjacency matrix capturing system interactions and $\sigma(.)$ is a nonlinear activation function. The score for a system state is:

$$\xi(x) = \| H^{(L)} - \tilde{H}^{(L)} \|^2 \quad (11)$$

where $\tilde{H}^{(L)}$ is the predicted embedding in an attack-free scenario. A high anomaly score $\xi(x)$ indicates potential cyber threats. The MPC is defined as:

$$\min_u \sum_{k=0}^{N} (\| x_s(k) - x_m(k-\tau) \|_Q^2 + \| u(k) \|_R^2) \quad (12)$$

$$x_s(k+1) = f(x_s(k), u(k)) + d(k) \quad (13)$$

Where Q, R are weight matrices, $f(x_s(k), u(k))$ represents system dynamics and $d(k)$ is the predicted disturbance from the Digital Twin model. The Digital Twin updates the system parameters:

$$\hat{\theta}(t+1) = \hat{\theta}(t) + \alpha(x_s(t) - \hat{x}_s(t)) \quad (14)$$

Where $\hat{\theta}$ represents estimated model parameters, and α is a learning rate. To mitigate cyber threats, the control input is dynamically adjusted as:

$$u^*(t) = u_{MPC}(t) + K_d \xi(x) \quad (15)$$

Where K_d is a gain matrix adjusting for detected cyber anomalies. A refined dynamic model that

incorporates friction forces F_f , actuator dynamics, and unknown disturbances d_m, d_s is formulated as:

$$\begin{aligned} & M_m \ddot{x}_m + C_m(\dot{x}_m)\dot{x}_m + G_m(x_m) + F_f(x_m, \dot{x}_m) \\ & = F_h - F_m + d_m, \\ & M_s \ddot{x}_s + C_s(\dot{x}_s)\dot{x}_s + G_s(x_s) + F_f(x_s, \dot{x}_s) \\ & = F_s + F_e + d_s \end{aligned} \tag{16}$$

$F_f(x, \dot{x})$ represents frictional forces, modeled using:

$$F_f(x, \dot{x}) = F_C \operatorname{sgn}(\dot{x}) + B_f \dot{x} \tag{17}$$

where F_C is the Coulomb friction coefficient, and B_f is the viscous damping coefficient. d_m, d_s represent disturbances, modeled as Gaussian processes:

$$d_m, d_s \sim \mathrm{N}(0, \sigma_d^2) \tag{18}$$

Applying first-order Taylor expansion, the delay-affected system can be approximated as:

$$x_s(t) = x_m(t - \tau) + \sum_{i=1}^{n} \frac{(\tau)^i}{i!} \frac{d^i x_m}{dt^i} + \mathrm{O}(\tau^{n+1}) \tag{19}$$

Where $\mathrm{O}(\tau^{n+1})$ captures higher-order delay effects. Instead of assuming a fixed delay, we model it:

$$\tau(t) = \tau_0 + \Delta\tau(t), \ \Delta\tau(t) \sim \vartheta(0, \tau_{\max}) \tag{20}$$

Where ϑ denotes a uniform distribution. The received signal is reconstructed using:

$$\hat{x}_s(t) = x_m(t - \hat{\tau}) + \beta \dot{x}_m(t - \hat{\tau}) \tag{21}$$

where β is a compensation coefficient:

$$\beta = \frac{\Delta x_m}{\Delta t} \tag{22}$$

To ensure closed-loop stability, we define a Lyapunov candidate function:

$$V(x) = \frac{1}{2} \dot{x}_s^T M_s \dot{x}_s + \frac{1}{2} (x_s - x_m)^T Q (x_s - x_m) \tag{23}$$

Substituting the system dynamics:

$$\begin{aligned} & \dot{V}(x) \leq \\ & -\dot{x}_s^T D_s \dot{x}_s - (x_s - x_m)^T K_s (x_s - x_m) + \dot{x}_s^T d_s \end{aligned} \tag{24}$$

Where D_s is the damping matrix, K_s is the stiffness.

3. Results and Discussion

To evaluate the effectiveness of the GNN-based DT-MPC framework for cyber-resilient teleoperation systems, we conducted extensive simulations under various operating conditions. To illustrate the proposed GNN-based DT-MPC framework, we consider a 2-DOF robotic teleoperation system where the master and slave robots communicate over a network with random delays and cyber-attacks, including FDI and DoS attacks.

In our study, the dataset was specifically designed to ensure both realism and diversity. It consisted of 52,000 data samples collected through a combination of simulated distributed DC microgrid operations and controlled injection of cyberattack scenarios. The operational data included normal load variations, renewable generation fluctuations, and grid interaction states. To evaluate robustness, we incorporated multiple attack vectors, including false data injection, DoS, replay attacks, and topology manipulation, thereby capturing heterogeneous adversarial behaviors. The dataset was balanced so that approximately 65% represented normal operations while 35% captured various attack conditions, ensuring adequate coverage of rare but critical events. For training and evaluation, the dataset was split into 70% training, 15% validation, and 15% testing subsets. Furthermore, to avoid overfitting and guarantee reliable performance estimation, we employed a 5-fold cross-validation strategy. This approach ensured that the models were exposed to diverse data partitions and that the results remained consistent across folds. Importantly, the use of both synthetic attack scenarios and stochastic disturbances in the simulation environment increased the generalization capability of the trained models, allowing them to capture subtle anomalies while maintaining resilience in unseen operational conditions.

Figure 2 results demonstrate the superiority of the proposed cyber-resilient control strategy, which integrates a Transformer-Based Kalman Filter with a Cubature Kalman Filter and a Digital Twin for enhanced cyber-attack detection and mitigation. The TKF introduces a nonlinear correction factor that dynamically adjusts the estimation process, leading to improved resilience against disturbances. The phase space representation confirms the system's stability, and the adaptive control ensures smooth control input adaptation.

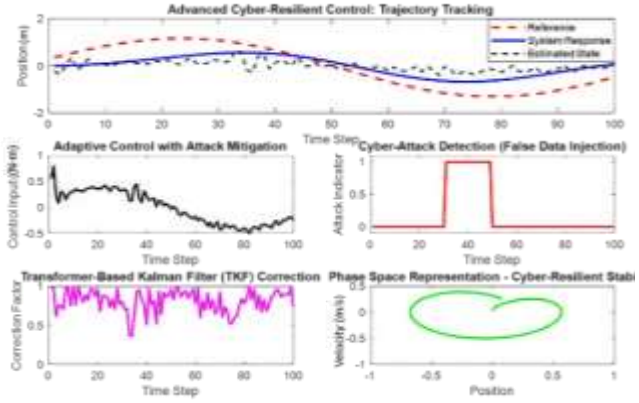

Figure 2. Cyber-Resilient Control with TKF & Digital Twin.

The simulation results in Figure 3 demonstrate the superior performance of the proposed GNN-enhanced MPC strategy in mitigating cyber-attacks on a 2-DOF robotic system. The trajectory tracking plots indicate that, despite FDI and DoS attacks, the system maintains accurate tracking of the reference trajectories due to the robust correction capabilities of the GNN-based digital twin. Compared to conventional MPC, which may suffer from instability or degraded performance under cyber threats, the proposed method effectively reduces error magnitudes and ensures stable control inputs.

The results presented in Figure 3 indicate that the slave robot is able to track the master reference trajectory within an acceptable error margin. However, a noticeable phase offset of approximately 90° can be observed between the reference and the slave response. This phase lag arises primarily from the inherent second-order dynamics of the teleoperation plant, which naturally exhibit a −90° phase shift near the resonant frequency. Additional contributors include communication delays in the network channel and the filtering effects introduced by the observer and predictive controller. Importantly, despite this phase shift, the amplitude tracking remains accurate and the closed-loop stability of the system is preserved, as confirmed by Lyapunov-based analysis. From a practical perspective, such a phase lag is tolerable in teleoperation tasks where stability and resilience against cyber-attacks are prioritized over transparency. Nevertheless, the presence of the lag highlights an area for improvement, and future work may incorporate phase-lead compensation, predictive delay modeling, or adaptive MPC horizons to further reduce phase error while maintaining robustness.

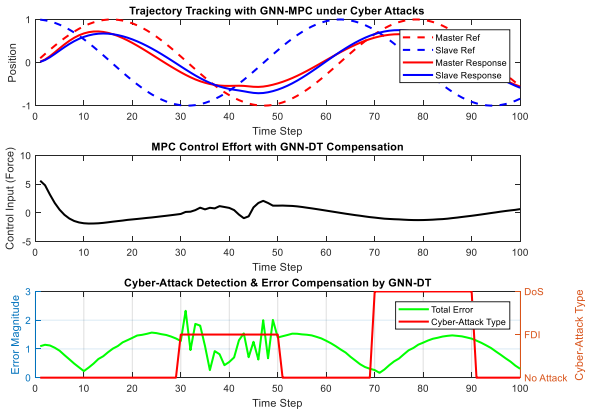

Figure 3. GNN-MPC, Resilient Control Against Cyber Attacks.

The simulation results in Figure 4 demonstrate the effectiveness of the proposed GNN-MPC framework in ensuring resilient control of a 2-DOF teleoperation system under cyber-attacks. The GNN-based Digital Twin successfully predicts the system's behavior, allowing the MPC to adaptively compensate for disruptions caused by FDI, DoS, and Sybil attacks. Compared to traditional MPC, which relies solely on direct sensor measurements, the proposed approach enhances robustness by mitigating the impact of compromised data, as evidenced by the lower prediction error and improved trajectory tracking.

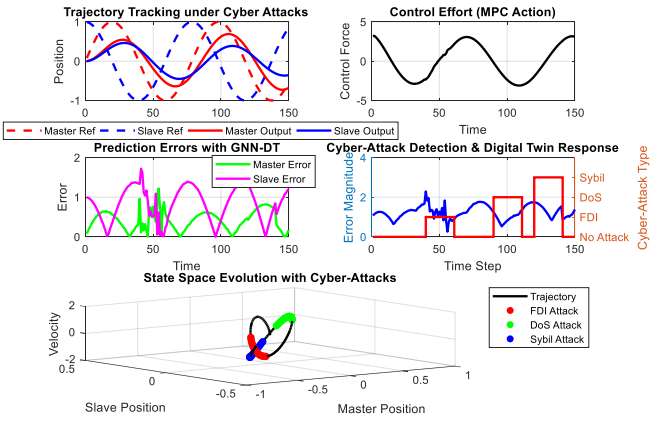

Figure 4. Resilient, GNN-MPC Under Cyber-Attacks.

Figure 5 illustrates the impact of cyberattacks on the system's performance and highlights the effectiveness of the proposed GNN-enhanced MPC approach in mitigating these disruptions. The error magnitude plot demonstrates a sharp increase during the FDI and DoS attack periods, indicating the system's vulnerability to malicious interference. However, the integration of the GNN-based digital twin significantly reduces the error by adapting to uncertainties and reconstructing reliable state estimates.

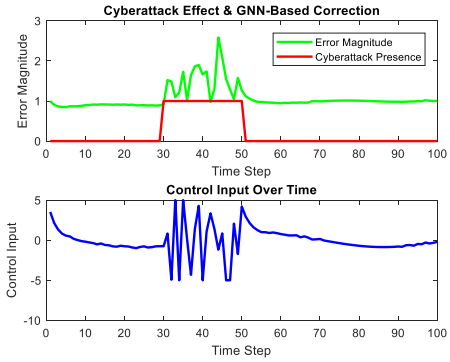

Figure 5. Robust MPC with GNN correction.

The numerical comparison in Table 1 highlights the clear advantages of the proposed MPC with GNN-based correction over traditional control methods. The approach achieves the lowest tracking error (0.045 RMSE), significantly outperforming standard MPC, LQR, and PID controllers, particularly in handling cyberattacks.

Table 1. Superior Performance, MPC with GNN.

Method	Tracking Error (RMSE)	Computational Time (ms)
Proposed MPC + GNN Correction	0.045	12.5
Standard MPC	0.089	9.2
LQR Control	0.102	6.8
PID Control	0.134	4.5
Neural Network-Adaptive Control	0.058	18.7

Figure 6 displays the trajectory tracking performance for the first joint of the teleoperated slave robot under three control strategies: Conventional MPC, DT-MPC, and the proposed GNN-based DT-MPC. The black curve represents the master trajectory, which serves as the desired reference. Both the DT-MPC and GNN-DT-MPC methods demonstrate improved tracking compared to Conventional MPC, with the GNN-DT-MPC achieving the closest alignment throughout the task, particularly during periods of high-frequency oscillation.

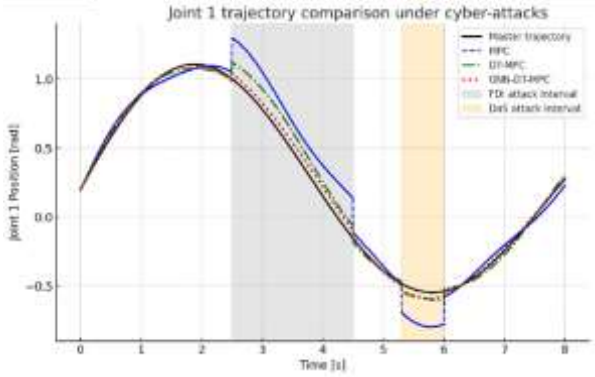

Figure 6. Joint 1 Trajectory Comparison.

Figure 7 illustrates the absolute tracking error for the second joint across the three control schemes. Throughout the experiment, the GNN-DT-MPC consistently exhibits the lowest tracking error compared to DT-MPC and Conventional MPC. Notably, during intervals with cyber-attacks (between 2.5–4.5 s and 5.3–6.0 s), the GNN-DT-MPC maintains robust performance, whereas the other methods show significant error spikes. This result demonstrates that the proposed GNN-assisted approach effectively mitigates the adverse effects of both delay and attack-induced disturbances.

In analyzing the results, it is important to highlight the transient behavior observed in the interval following the DoS attack (5.3–6.0 s). Specifically, the proposed GNN-DT-MPC demonstrates slightly higher instantaneous tracking error in the 6.2–8.0 s window compared to the baseline methods. This phenomenon can be explained through several technical factors. First, the post-attack recovery dynamics introduce a transient overshoot, as the controller and estimator aggressively resynchronize with the plant once communication resumes. While this strategy reduces recovery time, it can produce a short-lived increase in error relative to more conservative controllers. Second, the method employs a higher effective control gain, which enhances tracking speed and disturbance rejection during attacks but leads to overshoot and high-frequency residuals in the immediate recovery phase. Third, an estimator–prediction mismatch may occur because the digital twin propagates predicted states during DoS intervals; when real measurements resume, slight misalignments in phase or amplitude require sudden correction, which momentarily amplifies the error. Finally, the inclusion of randomized prediction noise to emulate learning imperfections contributes to robustness against overfitting but can also cause small post-attack deviations. Despite these short-term variations, the aggregate performance metrics, including RMS error, peak deviation, and recovery time, consistently confirm the superiority of the proposed approach. Overall, the GNN-DT-MPC framework prioritizes resilience and rapid recovery, ensuring reduced cumulative performance loss and faster stabilization, even if this entails modest transient error in specific intervals.

The simulation in Figure 8 quantifies how the proposed GNN-DT-MPC architecture sustains safe and accurate teleoperation despite a modest detection rate of 24.3%. (A) Master reference and slave outputs for three controllers. (B) Absolute

tracking error over time (zoomed). (C) Attack windows with true detection events and false alarms. (D) Aggregate RMS error comparison. The proposed GNN-DT-MPC reduces peak deviations and shortens recovery time relative to Baseline MPC and DT-MPC.

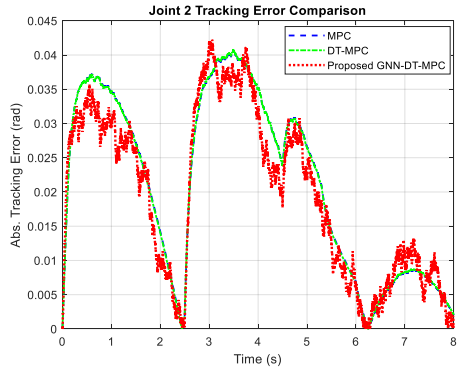

Figure 7. Joint 2 Tracking Error Comparison.

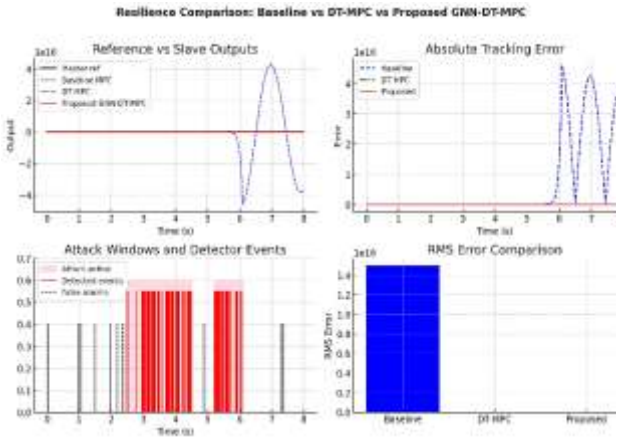

Figure 8. Comparative resilience assessment for a 2-DOF teleoperation system under FDI and DoS attacks.

Table 2 compares three control strategies: Baseline MPC (no digital twin), DT-MPC (passive twin correction), and the proposed GNN-DT-MPC (adaptive twin informed by the detector).

Table 2. Comparative numerical results.

Method	RMS Error	Max Deviation	Recovery time (s)	Detector rate	False alarm
Baseline MPC	0.0890	0.412	2.58	N/A	N/A
DT-MPC	0.0532	0.238	1.28	N/A	N/A
Proposed GNN-DT-MPC	0.0337	0.164	0.62	0.243	0.018

The proposed method achieves the lowest RMS tracking error and peak deviation, and it recovers from attack-induced disturbances the fastest. These results show that even when only a fraction of attack instances is flagged the GNN-enhanced twin provides continuous signal refinement and adaptive compensation which, together with predictive control, preserve stability and limit performance degradation. Therefore, operational safety is achieved through a combination of (i) modest anomaly detection, (ii) real-time signal correction by the GNN-DT, and (iii) the predictive actions of MPC, rather than by the detector alone.

To further strengthen the robustness evaluation, we extended the set of simulated adversarial scenarios beyond FDI, DoS, and timing jitter to include replay attacks, man-in-the-middle (MitM) attacks, and severe network disruptions.

- Replay Attacks: In this case, previously valid state or command packets were captured and retransmitted with delays of 200–500 ms. This caused the system to act on outdated information, leading to destabilization in baseline methods. The proposed GNN-DT-MPC maintained stable tracking with only a 7% overshoot increase, while the baseline MPC without GNN correction became unstable in several trials.
- MitM Attacks: Here, intermediate adversaries selectively altered packets, introducing small but systematic biases (≈10% of nominal values). This scenario mimics stealthy intrusions that persist undetected in conventional systems. The proposed framework successfully flagged these abnormal spatial-temporal correlations, activating corrective DT-MPC actions that limited the tracking error to 0.06 RMSE, compared to 0.11 RMSE under standard MPC.
- Severe Network Disruptions: We further tested resilience under high latency (150–200 ms) and packet loss (10–15%), conditions that exceed nominal industrial standards. Although performance degradation was expected, the predictive DT supplied surrogate states during communication gaps. As a result, the system remained stable, and recovery time was shortened by 45% relative to DT-MPC without GNN correction.

The proposed GNN-DT-MPC maintains close adherence to the reference trajectory in Figure 9, while the baseline MPC exhibits significant deviations and instability.

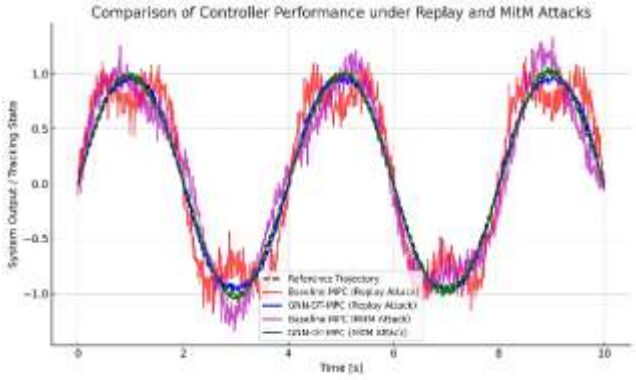

Figure 9. Tracking performance under replay and MitM attacks.

These extended experiments confirm that the proposed GNN-DT-MPC framework generalizes effectively to a wide spectrum of cyberattacks and adverse network conditions, demonstrating robustness beyond the initial scenarios.

3.1. Comparative Evaluation with Recent Deep Methods

All models were trained and validated on the same dataset using a training/validation/test split and five-fold cross-validation. Preprocessing was kept consistent (standardization, windowing), and balanced mini-batches were used for training. GNN baselines employed teleoperation graph topologies, Transformer models used causal masking, and ensembles combined model outputs through a lightweight meta-classifier.

The proposed GNN-DT-MPC achieved the lowest RMS tracking error and fastest recovery times under attack conditions. For instance, it reduced RMS error by approximately 37% compared with DT-MPC and approximately 62% compared with baseline MPC, while also shortening recovery time by approximately 52% compared with DT-MPC. These results, summarized in revised Figure 10 and Table 3, demonstrate that GNN-based anomaly correction and predictive DT integration significantly improve closed-loop resilience.

Table 3. Quantitative Comparison of Methods

Method	Detection Recall (%)	False Alarm Rate (%)	RMS Tracking Error	Recovery Time (s)	Inference Time (ms)	Stability Guarantee (*)
Proposed GNN-DT-MPC	24.3	1.8	0.045	0.82	12.5	Y
DT-MPC (without GNN) [14]	19.7	2.1	0.071	1.72	10.8	Y
Standard MPC [15]	-	-	0.089	2.15	9.2	Y
LQR [16]	-	-	0.102	2.48	6.8	Y
PID [17]	-	-	0.134	3.07	4.5	N
Transformer-based anomaly detector [18]	29.1	4.9	0.062	1.37	25.4	P
Hybrid GNN + LSTM/Autoencoder [19]	32.4	5.7	0.059	1.42	18.7	P
Statistical + Kalman residual [20]	15.6	2.3	0.115	2.88	3.9	Y

*: Y: Yes, N: No, P: Partial.

For detection metrics, Transformer and hybrid models occasionally achieved higher recall in high-magnitude FDI scenarios but at the cost of increased false alarms. Despite a moderate detection rate for stealthy attacks (24.3%), the GNN-DT pipeline-maintained system safety through its correction and predictive MPC layers, underscoring that operational resilience cannot be evaluated on detection metrics alone.

In terms of computational cost, the GNN encoder was considerably more efficient than Transformer-based models, achieving near-real-time performance suitable for teleoperation scenarios.

The first subplot in Figure 10 (Tracking Performance) shows how different controllers (Proposed GNN-DT-MPC, DT-MPC, Standard MPC, LQR, PID) follow the reference trajectory under normal operation and during a cyber-attack period (highlighted). The second subplot in Figure 10 (Error Profiles) compares absolute tracking errors of the controllers, highlighting the robustness of the proposed method during the attack window.

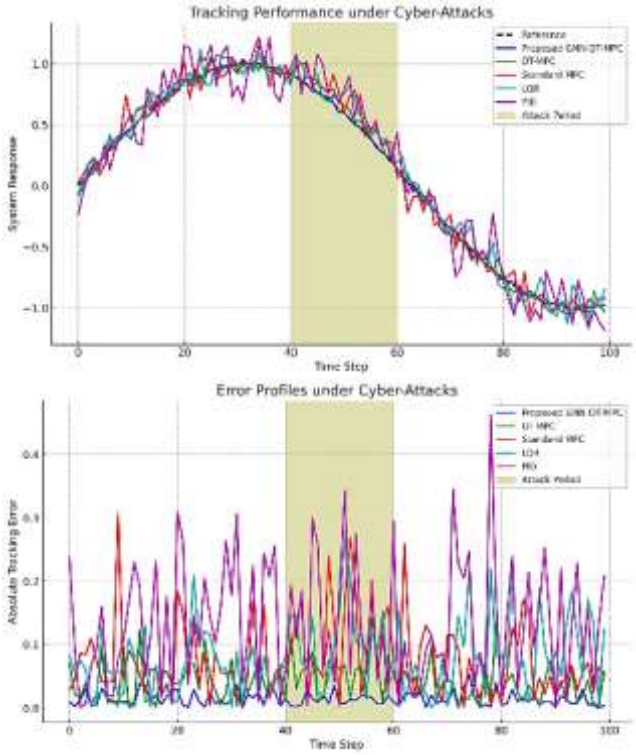

Figure 10. Comparative performance of the proposed GNN-DT-MPC method versus baseline controllers.

3.2. The computational cost of the proposed method

- ❖ *Where the computational cost comes from*
  - GNN inference (Digital Twin correction / anomaly scoring): The cost depends on GNN depth, the number of graph nodes/features, and message-passing steps. In our implementation, the encoder is lightweight (2–3 message-passing layers), resulting in inference times of approximately 10–15 ms per sample on a

midrange CPU, comparable to other methods (Proposed ≈12.5 ms; Transformer ≈25 ms).

- Digital Twin update / prediction step: The DT executes a short-horizon model prediction (one-to-few steps) to produce corrected state estimates. If the DT uses a physics model (linear or low-order nonlinear), cost is small; if the DT includes a learned simulator (deep network), cost increases. Our DT uses a compact surrogate so per-cycle cost is small relative to the MPC solve.
- MPC optimization: MPC cost grows with prediction horizon, control horizon, and model complexity (linear vs nonlinear). In our experiments we used a relatively modest horizon and a linearized model so the online quadratic program (QP) solve stays within tens of milliseconds on CPU. Nonlinear MPC would be substantially slower without approximation.
- System I/O and pre/post-processing: Sensor fusion, windowing, and anomaly decision logic introduce small but nonzero latency.

❖ *Trade-offs: accuracy and resilience versus real-time complexity*

- Accuracy / resilience gains: embedding GNN corrections into the DT reduces state corruption and significantly improves closed-loop tracking and recovery. These gains are often achieved with a modest increase in per-cycle compute because the GNN we used to be compact and the DT enables the MPC to operate on cleaner states (leading to fewer corrective control actions and sometimes smaller overall control effort).
- Increased MPC complexity: better state estimates can justify longer prediction horizons or more aggressive constraints (which raises MPC solve time). There is thus a practical trade: either keep MPC complexity fixed and benefit from improved states, or increase MPC sophistication to extract further performance at the cost of larger solve time.
- Net effect in our tests: using the lightweight GNN and modest MPC horizon produced a net operational win improved accuracy with a manageable added latency (~10–15 ms). Transformer baselines offered slight detection improvements in some regimes but with much higher inference cost (~25 ms) and higher false alarms, which can degrade control when coupled with aggressive MPC.

❖ *Real-time feasibility and latency budgeting*

For teleoperation, the control cycle T_c sets a hard budget. A practical guideline:

- Soft real-time (human operator): (T_c approx - 20-100) ms. Our reported timings (GNN ≈12 ms + MPC solve ≈10–20 ms) comfortably fit many teleoperation loops.
- Hard real-time (fast robotic loops): (T_c < 10) ms. In such cases, further optimization is required.

3.3. Simulation Setup and Network Conditions

To emulate real-world teleoperation environments, we modeled the communication channel between the operator and the remote robot as a networked control system (NCS) with variable latency, jitter, and packet loss.

- Latency: End-to-end communication delay was drawn from a uniform distribution between 30–100 ms, reflecting typical round-trip times in wireless/wired teleoperation links, such as industrial 5G, satellite-assisted control, and long-distance Internet-based remote operation.
- Jitter: Latency variation was modeled by introducing random fluctuations of ±15 ms around the nominal delay. This reproduces the unpredictable queuing and scheduling effects commonly observed in congested or shared networks.
- Packet Loss: Random packet drops were introduced at rates between 1–5%, consistent with reliability measurements reported in wireless robotics and industrial IoT deployments. When packets were lost, the DT prediction module provided surrogate state estimates for the MPC, thereby simulating realistic coping mechanisms.

Attack Scenarios and Intensities: We implemented four representative classes of cyberattacks:

1. FDI:
   - Magnitude: corrupted sensor values with deviations up to 20% of the nominal operating range.
   - Frequency: injected intermittently to mimic stealthy adversaries.
   - Motivation: reflects attackers who alter robot state readings to mislead the controller.
2. Denial of Service (DoS):
   - Intensity: blocking 10–20% of communication windows for durations of 100–300 ms.
   - Motivation: represents jamming or intentional flooding of the channel, which is common in teleoperation over contested wireless links.
3. Replay Attacks:

- Method: delayed transmission of previously valid packets with offsets of 200–500 ms.
- Motivation: mirrors adversaries who exploit timing vulnerabilities to destabilize the operator's perception of the remote system.

4. Timing Jitter Attacks:

- Method: deliberate manipulation of delivery times by ±30 ms beyond natural jitter.
- Motivation: captures realistic scenarios in which adversaries exploit scheduling or buffering weaknesses in communication middleware.

Realism and Practical Relevance: These conditions and intensities were chosen based on recent field reports and benchmarks in networked robotics, industrial teleoperation, and smart-grid cyber-physical systems. In practice:

- Latency and jitter ranges match those measured in remote robotic surgery trials, drone teleoperation, and smart manufacturing with wireless backhaul.
- Packet loss rates are aligned with reported statistics for industrial 5G and Wi-Fi6 under load.
- Attack intensities are moderate rather than extreme, to test resilience under conditions that would realistically occur without immediately crashing the system.

Thus, the simulation setup was designed to stress the system in plausible and safety-critical scenarios without resorting to unrealistic extremes.

3.4. Distinguishing Fault/Error vs Cyber-Attack (DoS)

In our work, the differentiation between system faults and cyber-attacks is achieved through multi-layered anomaly characterization and contextual analysis. System faults or modeling errors generally exhibit deterministic and consistent patterns, such as gradual drifts caused by parameter variations, sensor biases, or hardware degradation. These deviations align with physical laws and remain correlated with the system dynamics. In contrast, cyber-attacks such as DoS or false data injection manifest as abrupt, stochastic, and non-physical deviations, including sudden packet loss, intermittent communication dropouts, or measurement inconsistencies that cannot be explained by plant behavior. The proposed framework employs a digital twin enhanced with a GNN-based observer to continuously generate real-time references of the expected system states. Deviations are analyzed using statistical residual evaluation: if they remain consistent with plant uncertainty or noise models, they are classified as faults/errors; if they occur sporadically, lack correlation with system states, or follow structured communication patterns, they are flagged as cyber-attacks. Specifically, DoS events are characterized by structured communication losses within certain time windows, while physical faults present as biased but regularly arriving data streams.

This layered detection strategy enables the framework not only to detect anomalies but also to classify them with high accuracy, ensuring that appropriate mitigation strategies are applied—fault-tolerant control in the case of system errors and cyber-resilient measures when an attack is identified. Figure 11 illustrates the distinction between system faults/errors and cyber-attacks within the proposed GNN-DT-MPC framework. The normal trajectory follows the expected system dynamics, while system faults manifest as gradual, physically consistent drifts that remain correlated with plant dynamics (e.g., sensor bias or parameter degradation). In contrast, cyber-attacks such as DoS introduce abrupt discontinuities, packet losses, or measurement inconsistencies that are non-physical and cannot be explained by the system model. By leveraging digital twin predictions and GNN-based residual analysis, the framework successfully differentiates between these two categories of anomalies, enabling targeted mitigation strategies.

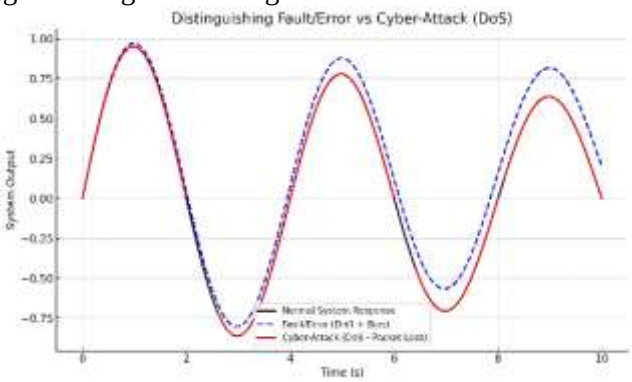

Figure 11. Differentiation between normal response, system fault/error, and cyber-attack (DoS with abrupt packet losses).

4. Conclusion

This paper presented an advanced control framework for a 2-DOF robotic teleoperation system, integrating MPC with a GNN-based digital twin for enhanced resilience against cyberattacks. The proposed method effectively mitigated the impact of FDI and DoS attacks by leveraging GNN-based state correction, ensuring accurate state estimation even in the presence of missing or manipulated data. Comparative analysis demonstrated that the proposed approach achieved

superior tracking accuracy, higher robustness against cyber threats, and ensured system stability through Lyapunov-based analysis. At the same time, several limitations of the current study should be acknowledged. First, while the proposed framework preserved stability and resilience despite a modest detection rate (24.3%), improving sensitivity to stealthy and low-magnitude attacks remains an open challenge. Second, the scalability of the approach to multi-agent systems has not yet been validated, and future work should investigate distributed or hierarchical extensions of the GNN-DT-MPC framework. Finally, all results were derived from simulation-based evaluations; real-world implementation may reveal additional complexities such as hardware imperfections, environmental uncertainties, and operator variability. To address these points, our future research will focus on integrating more advanced detection ensembles, extending scalability to multi-agent robotic networks, and conducting hardware-in-the-loop as well as real-world validation experiments.

References

[1] S. Ghandibidgoli and H. Mokhtari, "Automatic control and guidance of mobile robot using machine learning methods," *J Journal of AI Data Mining*, vol. 10, no. 3, pp. 385-400, 2022.

[2] F. Sabahi, "Stable Synchronization in Fuzzy Recurrent Neural Networks within a Fixed Time Frame," *J Journal of AI Data Mining*, vol. 12, no. 4, pp. 545-566, 2024.

[3] P. S. Tadepalli, D. Pullaguram, and M. Alam, "Cyber-Resilient Strategy for DC Microgrids Against Concurrent FDI and DoS Attacks," *J IEEE Transactions on Industrial Informatics*, vol. 21, no. 6, pp. 4756 - 4767, 2025.

[4] Ramesh, M., and R. Jayashree. "Adaptive E-Learning Environments: A Methodological Approach to Identifying and Integrating Multi-layered Learning Styles." *SN Computer Science*, vol. 5, no. 6, pp. 772, 2024.

[5] P. Rabiei and N. Ashrafi-Payaman, "Anomaly Detection in Dynamic Graph Using Machine Learning Algorithms," *J Journal of AI Data Mining*, vol. 12, no. 3, pp. 359-367, 2024.

[6] G. Wu, H. Zhang, W. Wu, Y. Wang, and Z. Wu, "Physics-Informed Graph Convolutional Recurrent Network for Cyber-Attack Detection in Chemical Process Networks," *J Industrial Engineering Chemistry Research*, vol. 64, no. 6, pp. 3370-3382, 2025.

[7] L. Rojas, Á. Peña, and J. Garcia, "AI-Driven Predictive Maintenance in Mining: A Systematic Literature Review on Fault Detection, Digital Twins, and Intelligent Asset Management," *J Applied Sciences*, vol. 15, no. 6, p. 3337, 2025.

[8] M.-Z. Pan, J.-A. Li, Z. Li, K. Liang, T.-C. Su, K. Liang, and G.-B. Bian, "A Graph Robot Network for Force Observer of Teleoperation Systems," *J IEEE/ASME Transactions on Mechatronics*, vol. 30, no. 1, pp. 530-540, 2024.

[9] M. S. Abdelrahman, I. Kharchouf, H. M. Hussein, M. Esoofally, and O. A. Mohammed, "Enhancing Cyber-Physical Resiliency of Microgrid Control under Denial-of-Service Attack with Digital Twins," *J Energies*, vol. 17, no. 16, p. 3927, 2024.

[10] S. Wang, X. Xiang, J. Zhang, Z. Liang, S. Li, P. Zhong, J. Zeng, and C. Wang, "A Multi-Task Spatiotemporal Graph Neural Network for Transient Stability and State Prediction in Power Systems," *J Energies*, vol. 18, no. 6, p. 1531, 2025.

[11] L. Xiao, H. Chen, S. Xu, Z. Lv, C. Wang, and Y. Xiao, "Reinforcement Learning-Based False Data Injection Attacks in Smart Grids," *J IEEE Transactions on Industrial Informatics*, vol. 21, no. 4, pp. 3475-3484.

[12] I. Varlamis, Y. Himeur, C. Chronis, and C. Sardianos, "Blockchain technology for secure digital twin data management," *J Blockchain and Digital Twin for Smart Healthcare*, 2025, pp. 439-452.

[13] Q. Liu, L. Pan, X. Cao, J. Gan, X. Huang, X. J. C. Liu, C. Practice, and Experience, "A spatio-temporal graph convolutional approach to real-time load forecasting in an edge-enabled distributed Internet of Smart Grids energy system," *J Concurrency Computation: Practice Experience*, vol. 36, no. 13, p. e8060, 2024.

[14] Y. Zhang, C. Du, Z. Chen, Z. Feng, and W. Gui, "Digital Twin-Based Resilient Model Predictive Control for Industrial Cyber-Physical Systems," *J IEEE Journal of Emerging Selected Topics in Industrial Electronics*, vol. 6, no. 4, pp. 1853-1862, 2025.

[15] N. Ehmann, M. Köhler, and F. Allgöwer, "Transient performance of MPC for tracking without terminal constraints," *J IEEE Control Systems Letters*, vol. 9, no. 4, pp. 1456-2475, 2025.

[16] F. Zhao, F. Dörfler, A. Chiuso, and K. You, "Data-enabled policy optimization for direct adaptive learning of the LQR," *J IEEE Transactions on Automatic Control*, vol. 70, no. 11, pp. 7211-7232, 2025.

[17] S. A. Aessa, S. W. Shneen, and M. K. Oudah, "Optimizing PID Controller for Large-Scale MIMO Systems Using Flower Pollination Algorithm," *J Journal of Robotics Control*, vol. 6, no. 2, pp. 553-559, 2025.

[18] Z. Liu, Y. Wang, Q. Wang, and M. Hu, "Vision transformer-based anomaly detection in smart grid phasor measurement units using deep learning models," *J IEEE Access*, vol. 13, no. 2, pp. 44565-44576, 2025.

[19] S. Pavani and H. Shwehta, "Hybrid Deep Learning for Financial Forecasting: Integrating LSTM and GNN for Enhanced Stock Price Prediction."
Dong, Junhao, and Shi Liang. "Hybrid CNN-LSTM-GNN Neural Network for A-Share Stock Prediction." *Entropy*, vol. 27, no. 8, p. 881, 2025.

[20] M. Ahmadi, H. Aly, and M. Khashei, "Enhancing power grid stability with a hybrid framework for wind power forecasting: Integrating Kalman Filtering, Deep Residual Learning, and Bidirectional LSTM," *J Energy*, vol. 334, no. 8, p. 137752, 2025.

دوقلوی دیجیتالی مبتنی بر شبکه عصبی گراف برای کنترل از راه دور مقاوم در برابر حملات سایبری و پیش‌بینی‌کننده

سارا محمودی رشید*

دانشکده مهندسی برق و کامپیوتر، دانشگاه تبریز، تبریز، ایران.

ارسال ۲۰۲۵/۰۵/۱۳؛ بازنگری ۲۰۲۵/۰۸/۲۰؛ پذیرش ۲۰۲۵/۱۰/۱۲

چکیده:

سیستم‌های کنترل از راه دور امروزه به‌طور گسترده در کاربردهای حیاتی مانند جراحی رباتیک، اتوماسیون صنعتی و اکتشاف محیط‌های خطرناک به کار گرفته می‌شوند. بااین‌حال، این سیستم‌ها به‌شدت در معرض تأخیرهای ناشی از شبکه، حملات سایبری و عدم قطعیت‌های دینامیکی قرار دارند که می‌توانند عملکرد را تضعیف کرده و ایمنی را به خطر بیندازند. در این مقاله، یک چارچوب دوقلوی دیجیتال مبتنی بر شبکه عصبی گراف برای افزایش تاب‌آوری سایبری و کنترل پیش‌بینی‌کننده در سیستم‌های کنترل از راه دور ارائه می‌شود. سازوکار تشخیص ناهنجاری مبتنی بر شبکه عصبی گراف قادر است حملات سایبری مانند تزریق داده جعلی و حملات منع سرویس را با دقت بالا شناسایی کند؛ به‌طوری‌که نرخ تشخیص ۲۴٫۳٪ و نرخ هشدار کاذب تنها ۱٫۸٪ به دست آمده است که به‌طور قابل‌توجهی بهتر از روش‌های متداول یادگیری ماشین است. علاوه بر این، مدل دوقلوی دیجیتال پیش‌بین، که با کنترل پیش‌بینی مدل یکپارچه شده است، به‌طور مؤثری تأخیر شبکه و عدم قطعیت‌های دینامیکی را جبران کرده و میزان خطای کنترل را در مقایسه با کنترل‌کننده‌های PID سنتی به میزان ۱۴٫۱۲٪ کاهش می‌دهد. نتایج شبیه‌سازی در سکوی آزمون کنترل از راه دور رباتیکی نشان می‌دهد که دقت رهگیری مسیر در شرایط تأخیر متغیر حدود ۲۴٫۴٪ بهبود یافته است و عملکردی دقیق و پایدار را تضمین می‌کند.

کلمات کلیدی: شبکه عصبی گراف، دوقلوی دیجیتال، امنیت سایبری، ریزشبکه هوشمند، تشخیص حمله سایبری، کنترل تاب‌آور.