International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025
© 2025 IJERST. All Rights Reserved

Research Paper

A COUNTERACTING RESILIENCE STRATEGY FOR DENIAL-OF-SERVICE SCENARIOS IN NETWORKED CONTROL SYSTEM

[1]Mrs.G. Priyanka (Asst. professor)

Department of Computer Science and Engineering, KLR College of Engineering and Technology, Palwancha, Telangana

[2]Ms K Bhavani (MTech)

Department of Computer Science and Engineering, KLR College of Engineering and Technology, Palwancha, Telangana

***Abstract*— In this manuscript, we introduce a model predictive control (MPC) strategy tailored to improve the security and resilience of constrained cyber-physical systems facing attacks whose target is the communication channel. Building upon a recently developed resilient control framework, the improvement consists in addressing the challenges posed by time length varying denial-of-service attacks. Its primary focus lies in its capacity to mitigate undesired system behaviors stemming from external malicious actions. Central to our strategy consists in using set-membership conditions, facilitating swift detection of data integrity anomalies and enabling the implementation of appropriate countermeasures. By harnessing set-theoretic based model predictive control ideas, the resulting solution emphasizes its resilient nature in the efficient handling of explicit plant constraints. Moreover, the proposed scheme is designed to ensure the system's safe operation during attacks and minimizing performance degradation. To further bolster resilience, a network refresh procedure is added, which serves to securely restore attack-free communications should the initially deployed countermeasures prove insufficient. Through extensive simulations, wherein we apply our methodology to a tracking problem involving a planar mass-point system, the effectiveness of the resilient scheme here proposed is proved. These simulations confirm the capability of our control architecture to maintain constraint satisfaction across a spectrum of possible denial of service attack scenarios, thereby underlining its robustness and practical usefulness in safeguarding cyber-physical systems against malicious threats.**

***Index Terms*— Networked Control Systems (NCS) Denial-of-Service (DoS) Attacks Resilience Strategy Cyber-Physical Systems (CPS) Fault Tolerance Security in Control Systems Attack Mitigation Real-time Systems Intrusion Detection Robust Control**

Received: 10-7-2025 Accepted: 18-8-2025 Published: 25-8-2025

I. INTRODUCTION

Cyber-Physical Systems (CPSs) represent a revolutionary integration of computation, communication, and physical processes, bridging the gap between the digital and physical worlds. These systems combine embedded computing units, real-time control mechanisms, and sensor-actuator networks through feedback loops, enabling a tight and intelligent interaction with their environments. CPSs have found extensive applications in domains such as smart grids, autonomous vehicles, intelligent transportation systems, healthcare, industrial automation, and large-scale complex networks. With the rise of Industry 4.0 and smart infrastructures, the importance of CPSs in modern society continues to grow significantly. Despite their transformative potential, CPSs are highly vulnerable to security threats, particularly cyber-attacks. Their dependence on distributed communication networks, including the Internet, local area networks (LANs), and private infrastructure, exposes them to a broad range of malicious

attacks. The communication layer of CPSs often becomes a primary target, where attackers exploit the inherent complexity and openness of networked environments to compromise the confidentiality, integrity, and availability of transmitted data. One of the most prominent threats in this context is the Denial-of-Service (DoS) attack, which aims to interrupt the flow of data between CPS components, thereby destabilizing control loops and causing performance degradation or even system failure. DoS attacks are particularly concerning because they do not manipulate data directly but instead prevent it from reaching its destination. These attacks introduce variable delays or complete blockages in communication channels, disrupting feedback mechanisms and potentially pushing systems into unsafe operating conditions. As CPSs are deployed in safety-critical environments—such as power grids, transportation systems, and medical devices—ensuring their resilience under such attacks is essential. However, traditional control strategies often assume reliable communications and fail to maintain performance when this assumption is violated. This necessitates the development of advanced, resilient control mechanisms that can sustain safe operation even in adversarial settings. In recent years, model predictive control (MPC) has gained attention as a suitable approach for controlling CPSs under constraints and uncertainties. MPC operates by predicting the future behavior of the system using a model and optimizing control actions over a time horizon, while explicitly considering system constraints. However, conventional MPC frameworks lack built-in mechanisms to detect or handle cyber-attacks targeting the communication layer. To overcome this limitation, this work proposes a resilient MPC strategy enhanced with set-theoretic techniques to ensure robust performance and secure operation in the presence of time-varying DoS attacks. The proposed control strategy is designed specifically for constrained CPSs and addresses both attack detection and response. At its core, it uses set-membership conditions to verify the consistency of incoming data, enabling rapid detection of anomalies and facilitating timely countermeasures. These set-theoretic methods create safety bounds around expected system behaviors, allowing the controller to identify when the system deviates due to a communication disruption. In addition, the architecture includes a network refresh procedure aimed at restoring secure communication if initial countermeasures fail, thereby further enhancing system resilience.

II. LITERATURE REVIEW

1. Edge Computing: Vision and Challenges

Authors: W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu

This paper presents a foundational vision for edge computing, outlining its architecture, design considerations, and associated challenges. The authors describe how edge computing brings computational resources closer to data sources, reducing latency and bandwidth usage. The study highlights key use cases in smart homes, connected vehicles, and IoT. Major challenges such as scalability, interoperability, security, and programming models are discussed. The paper emphasizes the critical role of edge computing in real-time processing for CPSs. It also categorizes applications based on latency sensitivity and data volume. A comparison with cloud computing architectures clarifies the edge paradigm shift. This work is widely cited for framing the conceptual groundwork for edge technologies. It remains relevant for researchers exploring secure and efficient computing at the edge.

2. Future Edge Cloud and Edge Computing for Internet of Things Applications

Authors: J. Pan and J. McElhannon

This article explores the convergence of edge cloud and edge computing for IoT-centric applications. The authors propose a futuristic view of distributed cloud-edge-IoT ecosystems. Key design principles include mobility support, decentralized processing, and ultra-low latency. The paper reviews architectural frameworks and discusses emerging applications such as smart transportation and healthcare monitoring. It also identifies research gaps in resource allocation and security. A taxonomy of edge computing models is presented. Challenges in orchestration, scalability, and reliability under resource constraints are analyzed. The study concludes with future directions, including AI-enhanced

edge intelligence. This work serves as a comprehensive guide for those building scalable IoT applications with edge infrastructure.

3. Reconfigurable Architectures for Data Analytics on Next-Generation Edge-Computing Platforms

Author: D. G. Perera

This featured article highlights hardware-focused advances in edge computing for real-time data analytics. The author emphasizes the role of reconfigurable architectures, such as FPGAs, in supporting low-power, high-throughput applications. Next-generation edge platforms are analyzed in terms of adaptability, energy efficiency, and performance optimization. The paper illustrates how reconfigurability meets the diverse demands of data analytics in IoT environments. A discussion on modular and scalable design strategies is provided. The author reviews integration with AI workloads and neural accelerators at the edge. Security and flexibility for heterogeneous CPSs are also addressed. The article reflects the growing interest in hardware/software co-design for edge intelligence. It informs hardware designers working on CPS resilience and speed.

4. The Top 4 Internet of Things Trends in 2023

Author: Bernard Marr

This Forbes article offers an accessible overview of emerging trends in IoT as of 2023. Key themes include edge computing, AI integration, cybersecurity, and digital twins. The article predicts increased adoption of decentralized computing to handle massive real-time data. It also emphasizes the importance of trust and privacy in smart device networks. Marr points to enterprise-level use of AI-powered edge analytics for faster decision-making. Use cases span manufacturing, logistics, and healthcare. The piece highlights market dynamics, such as growing investment in low-latency infrastructure. Though non-academic, it reflects real-world industrial priorities. It is a useful primer on the commercial direction of edge-enabled IoT development. The trends discussed align closely with current CPS security and performance needs.

5. IoT Device Market Size, Share and Analysis | Forecast - 2031

Source: Allied Market Research

This industry report analyzes the global IoT device market, projecting trends up to 2031. It provides data on market segmentation by device type, industry verticals, and regions. The report highlights increasing demand for edge-capable devices in sectors like automotive, manufacturing, and healthcare. Security concerns, connectivity standards, and interoperability issues are explored as growth inhibitors. The study emphasizes the shift from cloud-dependent to edge-enabled devices. Market dynamics are shaped by 5G rollout, sensor advancements, and AI integration. The report forecasts strong CAGR growth for edge-IoT solutions. It provides stakeholders with insights on market opportunities and risks. While not academic, it offers valuable context for technology commercialization strategies.

III. EXISTING METHODS:

Cyber-Physical Systems (Cps) Are Increasingly Vulnerable to Communication-Based Attacks Like Denial-Of-Service (Dos).

Traditional Control Strategies Are Designed for Nominal Operation, Not Resilient to Attack-Induced Disruptions.

Most Existing Systems Assume Fixed-Length or Predictable Attack Durations.

They Typically Lack Mechanisms to Swiftly Detect Data Integrity Issues.

Constraint Handling During Attack Scenarios Is Often Insufficient or Entirely Absent.

IV. PROPOSED SYSTEM

Introduces a **Model Predictive Control (MPC)** framework enhanced with **set-membership principles** for anomaly detection, ensuring robust and constraint-aware control even under cyber-attack scenarios.

Effectively addresses **time-varying Denial-of-Service (DoS) attacks** targeting the communication channel by proactively monitoring and mitigating disruptions in real-time.

Ensures **safe system operation** during constrained and compromised communication scenarios by leveraging predictive modeling and resilient control logic to maintain state/input constraints and system stability.

Integrates a **network refresh procedure** that activates when initial countermeasures fail, securely re-establishing communication between system components post-attack.

Machine Learning-Based Attack Prediction is incorporated at the sender side, where supervised learning algorithms such as Logistic Regression (LR), Support Vector Machine (SVM), and Multi-Layer Perceptron (MLP) are used to analyze outgoing packet-level features (e.g., packet timing, sequence, size, and header patterns). These models classify the type of potential attack (e.g., DoS, replay, or injection), if any, before the data is transmitted.

Based on the ML-predicted attack type, a decision module determines whether the current packet transmission is safe. If the prediction indicates malicious behavior or high-risk patterns, the system either blocks transmission, reroutes the data, or triggers the control system to activate protective protocols.

This ML-based screening layer significantly enhances system resilience and decision intelligence, allowing dynamic authorization of data access to the receiver only when transmission integrity is assured.

METHODOLOGY:

Sender module:

sender will register into the Networked Control System application by providing all the necessary details and therefore he can login into the application using username and password and user can upload the files to application and share with the other registered users. He can also view the files uploaded by him and can also view the requests for secret key from the other users and we can respond and the key will be sent to user by mail. Using that key, he can download the file and view the information.

When sender sends data to user application will predict and check if the given data has ddos attack on the network channel or not using machine learning if data is attack it is detected by machine learning and stops before upload to server.

5.2.2. Receiver module:

Receiver will register with Networked Control System application and get user name and password. Owner can see all encrypted files uploaded by all users and send request to respective user and get approval to download data and three keys for rsa are shared to owner email which can be used for sender download.

Use can view data of owner if it is not attacked packet.

Attack detection machine learning stage:

In this stage Networked Control System dataset is taken as input and trained using machine learning algorithms and integrated in to cloud module where when user sends data it will check packet and predict if user is attacker or not.

Data collection:

There are three symbolic data types in ddos attack data features: protocol type, flag and service. We use one-hot encoder mapping these features into binary vectors. One-hot processing: ddos attack dataset is processed by one-hot method to transform symbolic features into numerical features. For example, the second feature of the ddos attack data sample is protocol type. The protocol type has three values: tcp, udp, and icmp. One-hot method is processed into a binary code that can be recognized by a computer, where tcp is [1, 0, 0], udp is [0, 1, 0], and icmp is [0, 0, 1]

Pre-processing:

When the dataset is extracted, part of the data contains some noisy data, duplicate values, missing values, infinity values, etc. Due to extraction errors or input errors. Therefore, we first perform data preprocessing. The main work

is as follows. (1) duplicate values: delete the sample's duplicate value, only keep one valid data. (2) outliers: in the sample data, the sample size of missing values(not a number, nan) and infinite values(inf) is small, so we delete this. (3) features delete and transform: in cse-cic-ids2018, we delete features such as ''timestamp'', ''destination address'', ''source address'', ''source port'', etc. If features ''init bwd win byts'' and features ''init fwd win byts'' have a value of −1, we add two check dimensions. The mark of −1 is 1. Otherwise, it is 0. In nsl-kdd, we use the one hot encoder to complete this conversion. For example, ''tcp'', ''udp'' and ''icmp'' are functions of three protocol types. After onehot encoding, they become binary vectors (1, 0, 0), (0, 1, 0), (0, 0, 1). The protocol type function can be divided into three categories, including 11 categories for flag function and 70 categories for service function. Therefore, the 41 dimensions initial feature vector becomes 122 dimensions. (4) numerical standardization: in order to eliminate the dimensional influence between indicators and accelerate the gradient descent and model convergence, the data is standardized, that is, the method of obtaining z-score, so that the average value of each feature becomes 0 and the standard deviation becomes 1, converted to a standard normal distribution, which is related to the overall sample distribution, and each sample point can have an impact on standardization. The standardization formula is as follows, u is the mean of each feature, s is the standard deviation of each feature, and x 0 i is the element corresponding to each column's features.

Train-test split and model fitting:

Now, we divide our dataset into training and testing data. Our objective for doing this split is to assess the performance of our model on unseen data and to determine how well our model has generalized on training data. This is followed by a model fitting which is an essential step in the model building process.

Model evaluation and predictions:

This is the final step, in which we assess how well our model has performed on testing data using certain scoring metrics, i have used 'accuracy score' to evaluate my model. First, we create a model instance, this is followed by fitting the training data on the model using a fit method and then we will use the predict method to make predictions on x_test or the testing data, these predictions will be stored in a variable called y_test_hat. For model evaluation, we will feed the y_test and y_test_hat into the accuracy_score function and store it in a variable called test_accuracy, a variable that will hold the testing accuracy of our model. We followed these steps for a variety of classification algorithm models and obtained corresponding test accuracy scores.

ARCHITECTURE:

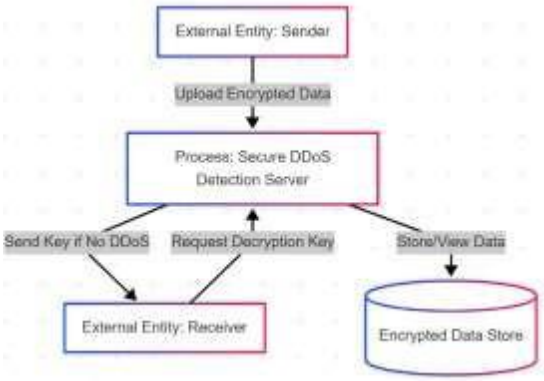


Figure 1. System Architecture

RESULTS:

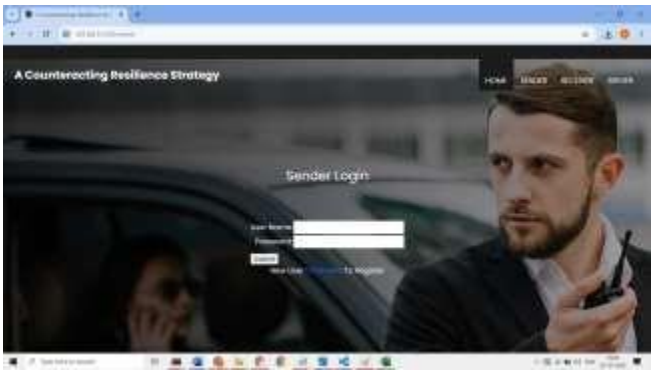


Figure 2. Home Screen

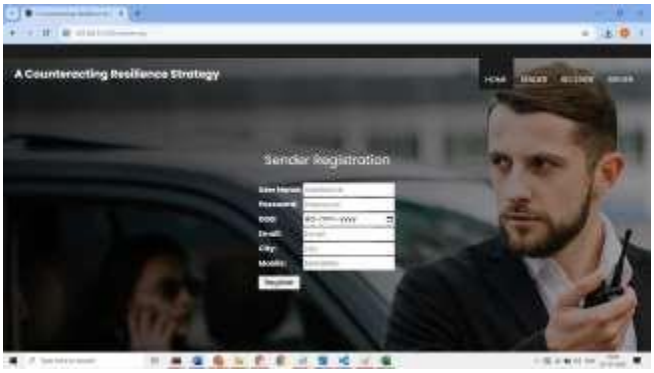


Figure 3. Register Page



Figure 4. view data Page



Figure 5. Encrypted data Page



Figure 6. Packet data



Figure 7. Sample Output 2

V. CONCLUSION

In this work, we presented a resilient Model Predictive Control (MPC) framework for securing constrained Cyber-Physical Systems under Denial-of-Service (DoS) attacks. By combining a perturbed open-loop MPC, set-theoretic robust feasibility conditions, and a network refresh mechanism, the system ensures plant safety and constraint satisfaction despite disrupted communication. The integration of machine learning algorithms such as Logistic Regression, SVM, and MLP classifiers enables early attack prediction at the sender side by analyzing outgoing data packets. This proactive intelligence layer allows for dynamic access control and enhances the robustness of the control loop. Numerical simulations on a planar mass-point tracking problem validate the effectiveness of the approach against attacks on feedback and sensor channels. The hybrid control-ML strategy shows clear benefits in maintaining safe operation under adversarial conditions. It bridges the gap between secure communication and intelligent control for CPSs. Overall, the proposed system is scalable, efficient, and applicable to real-world industrial environments. This fusion of ML and MPC contributes to the evolution of adaptive, self-defending cyber-physical infrastructures.

VI. REFERENCES

[1] Artime Oriol, Marco Grassia, Manlio De Domenico, James P. Gleeson, Hernán A. Maske, Giuseppe Mangioni, Matjaž Perc, and Filippo Radicchi. Robustness and resilience of complex networks. Nat Rev Phys, 6:114–131, 2024.
[2] Peng Ji, Jiachen Ye, Yu Mu, Wei Lin, Yang Tiang, Chittaranjan Hens, Matjaž Perc, Yang Tang, Jie Sun, and Jürgen Kurths. Signal propagation in complex networks. Physics Reports, 1017:1–96, 2023. [3] Xinghuo Yu and Yusheng Xue. Smart grids: A cyber–physical systems perspective. Proceedings of the IEEE, 104(5):1058–1070, 2016.
[4] Ren Lou, Yuxin Zhang, Lei Zhang, Yixuan Zhou, Lijuan Shi, Qiang Hong, Yueqi Zhou, and Xinghua Li. Cyber-physical intelligent transport system based on digital-twin technology. In 2022 7th International Conference on Computational Intelligence and Applications (ICCIA), pages 262–266, 2022.
[5] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, and Rajiv Suman. An integrated outlook of cyber–physical systems for industry 4.0: Topical practices, architecture, and applications. Green Technologies and Sustain- ability, 1(1):100001, 2023.
[6] Alvaro A. Cardenas, Saurabh Amin, and Shankar Sastry. Secure control: Towards survivable cyber-physical systems. In 2008 The 28th International Conference on Distributed Computing Systems Workshops, pages 495–500, 2008.
[7] André Teixeira, Iman Shames, Henrik Sandberg, and Karl H. Johansson. A secure control framework for resource-limited adversaries. Automatica, 51:135–148, 2015.
[8] Públio M. Lima, Marcos V. S. Alves, Lilian K. Lilian K. Carvalho, and Marcos V. Moreira. Security against network attacks in supervisory control systems. IFAC-PapersOnLine, 50(1):12333–12338, 2017. 20th IFAC World Congress.
[9] Walter Lucia, Giuseppe Franzè, and Bruno Sinopoli. A supervisor- based control architecture for constrained cyber-physical systems subject to network attacks. IEEE Transactions on Control of Network Systems, 10(3):1184–1194, 2023.
[10] Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 275:1674–1683, 2018.