International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

INVARIANT BASED CYBER ATTACK DETECTION IN MANUFACTURING CPS

Varsha[1], Karanam Harish[2] ,T.Nivesh Reddy[3] , K. Surya Kanthi[4]
[1,2,3] UG Scholar, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
varsha1237varsha@gmail.com

Abstract:

The era of the Industrial Internet of Things has led to an escalating menace of cyber–physical manufacturing systems (CPMSs) to cyber-attacks. Presently, the field of intrusion detection for CPMS has significant advancements. However, current methodologies require significant costs for collecting historical data to train detection models, which are tailored to specific machining scenarios. Evolving machining scenarios in the real world challenge the adaptability of these methods. In this article, We found that the machining code of the CPMS contains a complete machining process, which is an excellent detection basis. Therefore, we propose MPI-CNC, an intrusion detection approach based on Machining Process Invariant in the machining code. Specifically, MPI-CNC automates the analysis of the machining codes to extract machining process rules and key parameter rules, which serve as essential detection rules. Then, MPI-CNC actively acquires runtime status from the CPMS and matches the detection rules to identify cyberattacks behavior. MPI-CNC was evaluated using two FANUC computer numerical control (CNC) machine tools across ten real machining scenarios. The experiment demonstrated the exceptional adaptability capability of MPI-CNC. Furthermore, MPI-CNC showed superior accuracy in detecting cyber-attacks against CPMS compared to existing state-of-the-art detection methods while ensuring normal machining operations. Index Terms—Computer numerical control (CNC), cyber attack, cyber–physical manufacturing systems (CPMSs), Industrial Internet of Things, intrusion detection

Tesla's Giga factory connects CNC systems to the industrial Internet to automatically control production processes, greatly improving production efficiency.

Keywords : Cyber-Attack Detection, Machining Process Invariant, MPI-CNC, Intrusion Detection, Machining Code Analysis, Detection Rules, Security Exploitation, Network Security

1. INTRODUCTION

The rapid advancement of the Industrial Internet of Things (IIoT) has transformed the landscape of modern manufacturing, integrating networked cyber-physical manufacturing systems (CPMSs) with intelligent automation. While this evolution has enhanced efficiency and precision, it has also exposed CPMSs to an increasing number of cyber threats. The growing reliance on computer numerical control (CNC) systems, which play a critical role in industries such as aerospace, automotive, and defense, makes the security of these systems a paramount concern Cyber-attacks targeting CPMSs can have devastating consequences, ranging from operational disruptions to compromised product integrity and potential safety hazards. Traditional intrusion detection methodologies rely heavily on historical data to train anomaly detection models, but these approaches are often limited by their high cost, slow adaptability to evolving machining environments, and inability to detect novel threats effectively. Additionally, the dynamic nature of manufacturing scenarios presents significant,An increasing number of factories integrate their CNC systems into the Industrial Internet, the security of CPMS has become a paramount requirement and faces formidable challenges. Intrusion detection approaches for CPMS have emerged as a prominent and burgeoning topic. Currently in the field of CPMS security, most researchers focus on training machine learning classification models to detect anomalies by analyzing side channel data, such as current , video , or audio , generated during machining. Some researchers have built digital twin models for CNC systems with a data-driven approach to do consistency checks on the runtime state of CNC systems to detect cyber-attacks . There is also an offline approach to detect whether machining codes have been tampered with, which extracts digital features of machining codes and trains machine learning anomaly classification models . These solutions can effectively detect anomalous processing behaviors for specific machining sce narios.In practical production processes, the CNC system employs various machining codes to handle different products, leading to diverse machining scenarios. These dif ferent scenarios require distinct tool paths, raw materials, and machining tools, resulting in different side-channel features with audio, image, current, and voltage. To develop intrusion detection models using side-channel data across different machining scenarios, researchers typically need to gather side channel data for each new scenario and repeat the training process, incurring significant time and labor costs. However, once attackers successfully deploy an attack script in a CPMS system, they can easily disrupt the different machining scenarios. The effectiveness of MPI-CNC was evaluated through experiments conducted on two

FANUC CNC machine tools, covering ten distinct machining scenarios and multiple cyber-attack vectors.

2. LITERATURE SURVEY

1. Stealthy Cyber Anomaly Detection On Large Noisy Multi- material 3D Printer Datasets Using Probabilistic Models

As Additive Layer Manufacturing (ALM) becomes pervasive in industry, its applications in safety critical component manufacturing are being explored and adopted. However, ALM's reliance on embedded computing renders it vulnerable to tampering through cyber-attacks. Sensor instrumentation of ALM devices allows for rigorous process and security monitoring, but also results in a massive volume of noisy data for each run. As such, in-situ, near-real-time anomaly detection is very challenging. The ideal algorithm for this context is simple, computationally efficient, minimizes false positives, and is accurate enough to resolve small deviations. In this paper, we present a probabilistic- model-based approach to address this challenge. To test our approach, we analyze current measurements from a polymer composite 3D printer during emulated tampering attacks. Our results show that our approach can consistently and efficiently locate small changes in the presence of substantial operational noise.

2. Securing cyber-physical additive manufacturing systems by *in-situ* process authentication using streamline video analysis

In cyber-physical systems (CPS) of additive manufacturing (AM), cyber-attacks may significantly alter the design of the AM part, compromising its mechanical properties and functionalities. *In- situ* process authentication may assure that the AM part is fabricated as intended. Most cyber-physical attacks towards AM processes can be manifested as printing path alterations, and an *in- situ* optical imaging system can detect alteration in the printing path. This will prevent catastrophic geometric changes and mechanical property compromises in the AM parts, ultimately improving the AM process security. In this paper, a novel process authentication methodology is proposed based on image texture analysis of the layer-wise *in-situ* videos. The layer-wise distribution of the segmented textures' geometric features is characterized as the layer-wise texture descriptor tensor (LTDT). Given the high dimensionality and sparsity of the extracted LTDTs, the multilinear principal component analysis (MPCA) algorithm is used for dimension reduction. Subsequently, the Hotelling T2 control charting technique is adopted for alteration detection based on the extracted low-dimensional layer-wise features. Case studies based on a fused filament fabrication (FFF) process were conducted to evaluate and validate the proposed framework. The proposed method can achieve over 95% of accuracy, which illustrates that the proposed method can accurately detect process alterations due to printing path changes. In addition, the proposed method significantly outperforms the benchmark method. The computation time for both the proposed and benchmark method is also compared.

3. KCAD: Kinetic Cyber-attack detection method for Cyber- physical additive manufacturing systems

Additive Manufacturing (AM) uses Cyber-Physical Systems (CPS) (e.g., 3D Printers) that are vulnerable to kinetic cyber- attacks. Kinetic cyber-attacks cause physical damage to the system from the cyber domain. In AM, kinetic cyber-attacks are realized by introducing flaws in the design of the 3D objects. These flaws may eventually compromise the structural integrity of the printed objects. In CPS, researchers have designed various attack detection method to detect the attacks on the integrity of the system. However, in AM, attack detection method is in its infancy. Moreover, analog emissions (such as acoustics, electromagnetic emissions, etc.) from the side-channels of AM have not been fully considered as a parameter for attack detection. To aid the security research in AM, this paper presents a novel attack detection method that is able to detect zero-day kinetic cyber-attacks on AM by identifying anomalous analog emissions which arise as an outcome of the attack. This is achieved by statistically estimating functions that map the relation between the analog emissions and the corresponding cyber domain data (such as G-code) to model the behavior of the system. Our method has been tested to detect potential zero-day kinetic cyber-attacks in fused deposition modeling based AM. These attacks can physically manifest to change various parameters of the 3D object, such as speed, dimension, and movement axis. Accuracy, defined as the capability of our method to detect the range of variations introduced to these parameters as a result of kinetic cyber-attacks, is 77.45%.

4. Digital Audio Signature for 3D Printing Integrity

Additive manufacturing (AM, or 3D printing) is a novel manufacturing technology that has been adopted in industrial and consumer settings. However, the reliance of this technology on computerization has raised various security concerns. In this paper, we address issues associated with sabotage via tampering during the 3D printing process by presenting an approach that can verify the integrity of a 3D printed object. Our approach operates on acoustic side-channel emanations generated by the 3D printer's stepper motors, which results in a non-intrusive and real-time validation process that is difficult to compromise. The proposed approach constitutes two algorithms. The first algorithm is used to generate a master audio fingerprint for the verifiable unaltered printing process. The second algorithm is applied when the same 3D object is printed again, and this algorithm validates the monitored 3D printing process by assessing the similarity of its audio signature with the master audio fingerprint. To evaluate the quality of the proposed thresholds, we identify the detectability thresholds for the following minimal tampering primitives: insertion, deletion, replacement, and modification of a single tool path command. By detecting the deviation at the time of occurrence, we can stop the printing process for compromised objects, thus saving time and preventing material waste. We discuss various factors that impact the method, such as background noise, audio device changes, and different audio recorder positions.

5. Digital-twin-based testing for cyber–physical systems: : A systematic literature review

Cyber–physical systems present a challenge to testers, bringing complexity and scale to safety-critical and collaborative environments. Digital twins enhance these systems through data-driven and simulation based models coupled to physical systems to provide visualisation, predict future states and communication. Due to the coupling between digital and physical worlds, digital twins provide a new perspective into cyber–physical system testing.The objectives of this study are to summarise the existing literature on digital-twin-based testing. We aim to uncover emerging areas of adoptions, the testing techniques used in these areas and identify future research areas.We conducted a systematic literature review which answered the following research questions: What cyber–physical systems are digital twins currently being used to test? How are test oracles defined for cyber–physical systems? What is the distribution of white-box, black-box and grey-box modelling techniques used for digital twins in the context of testing? How are test cases defined and how does this affect test inputs,We uncovered 26 relevant studies from 480 produced by searching with a curated search query. These studies showed an adoption of digital-twin- based testing following the introduction of digital twins in industry as well as the increasing accessibility of the technology. The oracles used in testing are the digital twin themselves and therefore rely on both system specification and data derivation. Cyber–physical systems are tested through passive testing techniques, as opposed to either active testing through test cases or predictive testing using digital twin prediction.

6. Does Explicit Information Security Policy Affect Employees

Research on the impact of explicit information security policies on employees' cybersecurity behavior suggests that clear, well-communicated policies can significantly influence how employees adhere to security practices. A pilot study on this topic indicates that when employees are aware of specific security guidelines, they are more likely to engage in protective behaviors such as using strong passwords, avoiding phishing scams, and following data protection protocols. However, the study also emphasizes that the mere existence of a security policy is not enough. The effectiveness depends on factors such as policy clarity, organizational culture, and continuous training. Employees' understanding and perception of these policies play a critical role in shaping their cyber hygiene and reducing human-related security vulnerabilities.

7. Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud

The integration of Industry 4.0 technologies, such as the Industrial Control Systems (ICS), artificial intelligence (AI), and cloud computing, has transformed industrial operations but also introduced new cybersecurity risks. Studies utilizing ICS testbeds for cybersecurity risk assessment in Industry 4.0 environments emphasize the need for enhanced security measures to address these risks. AI-driven models are being employed to detect anomalies and predict potential cyber threats in real time, while cloud-based solutions offer scalable security management. However, research highlights vulnerabilities in data transmission, cloud infrastructure, and remote access, which can be exploited by cyber-attacks. These assessments provide critical insights into developing robust, AI-powered cybersecurity frameworks that can effectively safeguard Industry 4.0 systems against emerging threats. **O**rganizations are investing a lot of time and effort to develop their security policies and procedures which if not developed correctly, will lead to security vulnerabilities. AI proves itself as an effective mechanism to help generate these policies. It also helps to keep these policies on high standards and up to date, periodically revised and synchronized with the new published frameworks.

3. PROPOSED METHODOLOGY

The proposed system, MPI-CNC, introduces an advanced intrusion detection framework for cyber-physical manufacturing systems (CPMSs). This system is designed to enhance security by leveraging the inherent invariants within machining processes. The methodology is divided into three main components: Detection Rule Generation, Low-Interference Data Acquisition, and Active Anomaly Detection.

1. Detection Rule Generation

The first step in MPI-CNC is the automatic extraction of machining process invariants from CNC machining codes. These codes contain comprehensive information about machining trajectories, spindle speeds, feed rates, and tool changes. By analyzing these codes, the system generates detection rules that act as a baseline for identifying anomalies in real-time operations.

The generated detection rules include:

Machining Process Rules: Defines expected tool paths and machining behavior.

Key Parameter Rules: Establishes constraints on parameters such as feed rates and spindle speeds.

Whitelist-Based Filtering: Ensures only valid machining commands are executed.

By using these predefined rules, MPI-CNC avoids the limitations of traditional machine learning-based detection methods, which require

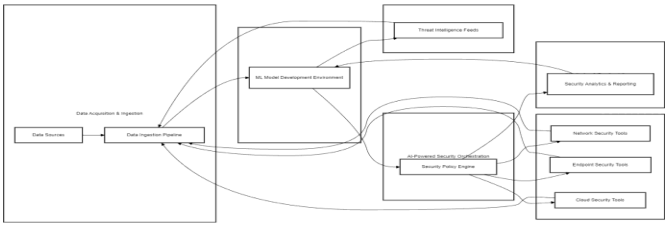

Data Acquisition & Ingestion
Data Sources
Data Ingestion Pipeline
ML Model Development Environment
Threat Intelligence Feeds
Security Analytics & Reporting
AI-Powered Security Orchestration
Security Policy Engine
Network Security Tools
Endpoint Security Tools
Cloud Security Tools

Figure1. Proposedn System.

2. Low-Interference Data Acquisition

To ensure efficient real-time monitoring, MPI-CNC employs a low- interference data acquisition strategy. Traditional monitoring techniques can introduce network latency and computational overhead, disrupting normal machining operations. To counter this, MPI-CNC utilizes optimized request packets that minimize network congestion while collecting real-time machining data.

The key features of this phase include:

Reverse Engineering of CNC Communication Protocols: Optimized data acquisition from FANUC and other CNC systems.

Low-Overhead Packet Transmission: Ensures real-time data collection without interfering with machining performance.

Adaptive Sampling Rates: Adjusts monitoring frequency based on the sensitivity of the detected process .These strategies allow MPI-CNC to gather crucial machining parameters without imposing significant computational loads on CNC systems.

3. Active Anomaly Detection

Once real-time machining data is collected, MPI-CNC performs active anomaly detection by comparing observed machining behavior against predefined detection rules. The system continuously verifies machining process consistency and detects potential cyber-attacks.

Real-Time Parameter Matching: Compares runtime data against key parameter rules.

Dynamic Time Warping (DTW) Analysis: Aligns real-time machining sequences with expected patterns.

Consistency Verification: Identifies unauthorized modifications to machining trajectories or execution parameters. By actively monitoring runtime behavior, MPI-CNC provides a robust detection mechanism capable of identifying attacks such as:

Machining Code Injection: Unauthorized modifications to CNC code execution.

Parameter Manipulation: Alteration of key machining parameters to introduce defects.

Instruction Injection: Execution of unauthorized control commands that disrupt production.

98.81% Accuracy in Attack Detection: Outperforming traditional side-channel analysis and digital twin-based detection methods.
Minimal Network Interference: Optimized data acquisition reduced network congestion by 38.41%.
Real-Time Monitoring Without Delays: Low-latency detection ensured rapid response to cyber threats

4. EXPERIMENTAL ANALYSIS

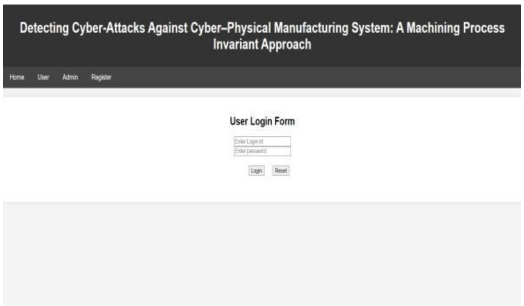

Detecting Cyber-Attacks Against Cyber–Physical Manufacturing System: A Machining Process Invariant Approach

Figure 1: User Login Page

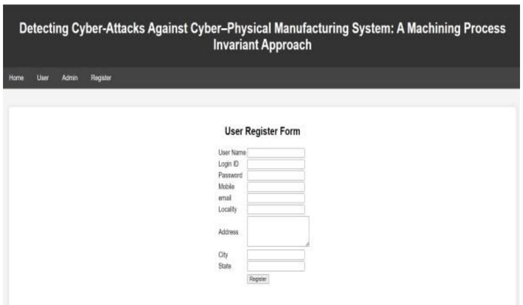

Detecting Cyber-Attacks Against Cyber–Physical Manufacturing System: A Machining Process Invariant Approach

Figure2: User Registration Form

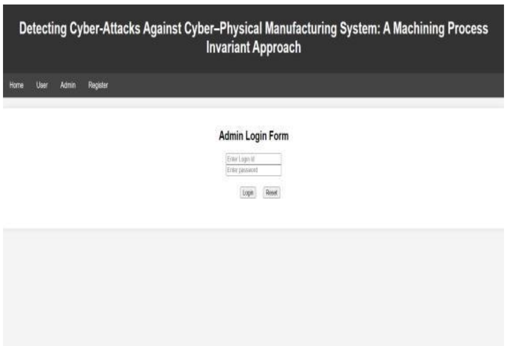
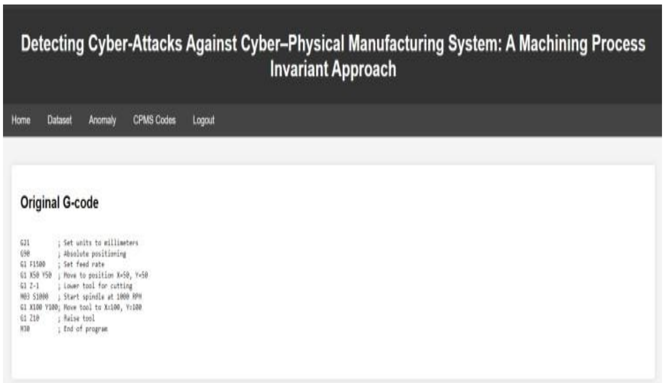

Detecting Cyber-Attacks Against Cyber–Physical Manufacturing System: A Machining Process Invariant Approach

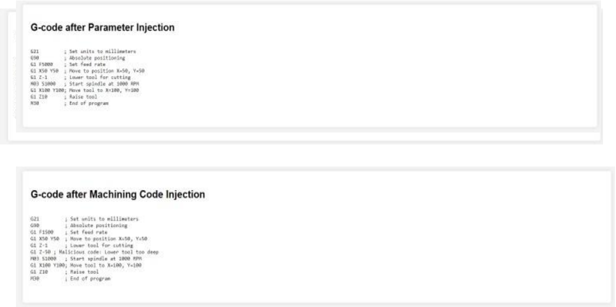
Figure 3: Admin Login Page


Detecting Cyber-Attacks Against Cyber–Physical Manufacturing System: A Machining Process Invariant Approach

Original G-code

```
G21         ; Set units to millimeters
G90         ; Absolute positioning
G1 F1500    ; Set feed rate
G1 X50 Y50  ; Move to position X=50, Y=50
G1 Z-1      ; Lower tool for cutting
M03 S1000   ; Start spindle at 1000 RPM
G1 X100 Y100; Move tool to X=100, Y=100
G1 Z10      ; Raise tool
M30         ; End of program
```

Figure 4: Original G-code


G-code after Parameter Injection

```
G21         ; Set units to millimeters
G90         ; Absolute positioning
G1 F5000    ; Set feed rate
G1 X50 Y50  ; Move to position X=50, Y=50
G1 Z-1      ; Lower tool for cutting
M03 S1000   ; Start spindle at 1000 RPM
G1 X100 Y100; Move tool to X=100, Y=100
G1 Z10      ; Raise tool
M30         ; End of program
```

G-code after Machining Code Injection

```
G21         ; Set units to millimeters
G90         ; Absolute positioning
G1 F1500    ; Set feed rate
G1 X50 Y50  ; Move to position X=50, Y=50
G1 Z-1      ; Lower tool for cutting
G1 Z-50 ; Malicious code: Lower tool too deep
M03 S1000   ; Start spindle at 1000 RPM
G1 X100 Y100; Move tool to X=100, Y=100
G1 Z10      ; Raise tool
M30         ; End of program
```

Figure 4: Types Of Injections

5. CONCLUSION

The proposed MPI-CNC system presents a scalable and effective solution for protecting CPMSs against cyber-attacks. By leveraging machining process invariants, MPI-CNC eliminates the dependency on historical datasets and enhances adaptability across different machining environments.

Future enhancements will focus on expanding compatibility with additional CNC systems and improving detection models through adaptive learning mechanisms. Additionally, research into automated protocol reversal methods will be explored to further optimize data acquisition and detection efficiency. Addressing challenges such as firmware-based man-in-the-middle attacks and expanding detection frameworks for five-axis machine centers will be key areas of development.

6. REFERENCES

[1] R. E. Baker, A. S. Mahmud, I. F. Miller, M. Rajeev, F. Rasambainarivo,B.L.Rice,S.Takahashi,A.J.Tatem,C.E.Wagner, L.-F. Wang et al., ―Infectious disease in an era of global change,‖ Nature Reviews Microbiology, vol. 20, no. 4, pp. 193–205, 2022.

[2] P.Ma,C.Li,M.M.Rahaman,Y.Yao,J.Zhang,S.Zou,X.Zhao, and M. Grzegorzek, ―A state-of-the-art survey of object detection techniques in microorganism image analysis: from classical methods to deep learning approaches,‖ Artificial Intelligence Review, vol. 56, no. 2, pp. 1627–1698, 2023.

[3] W.Liu,D.Anguelov,D.Erhan,C.Szegedy,S.Reed, C.-Y. Fu,and A.C.Berg,―Ssd:Singleshotmultiboxdetector,‖inComputerVision ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part I 14. Springer, 2016,pp.21–37.

[4] G. Haddad, S. Bellali,T.Takakura,A. Fontanini,Y. Ominami, J. BouKhalil,andD.Raoult,―Scanningelectronmicroscope:anew

[5] M. Bonnet, J. C. Lagier, D. Raoult, and S. Khelaifia, ―Bacterial culture through selective and non-selective conditions: **the evolution** of culture media in clinical microbiology,‖ New microbes and new infections, vol. 34, p. 100622, 2020.

[6] M.Ferone,A.Gowen,S.Fanning,andA.G.Scannell,―Microbial detec tion and identification methods: Bench top assays to omics approaches,‖ Comprehensive Reviews in Food Science and Food Safety, vol. 19, no. 6, pp. 3106–3129, 2020.

[7] A. Pathak, ―Fluorimetric and impedimetric sensors for the detection of pathogenic bacteria using carbon dots.‖

[8] J. D. Kaunitz, ―The discovery of pcr: Procurement of divine power,‖Digestivediseasesandsciences,vol.60,no.8,pp.2230–2231, 2015.

[9] V. Sankarapandian, K. Nitharsan, K. Parangusadoss, P. Gangadaran, P. Ramani,B.A.Venmathi Maran, and M. P. Jogalekar, ―Prebiotic potential and value-added products derived from spirulina laxissimasv001—asteptowardshealthyliving,‖BioTech,vol.11,no. 2, p. 13, 2022.

[10] S.RemyaandT.Anjali,―Anintelligentandoptimaldeeplearning approach in sensor based networks for detecting microbes,‖ IEEE Sensors Journal, 2023.

[11] S. Sadanandan, K. Ramkumar, N. P. Pillai, P. Anuvinda, V. Devika, K. Ramanunni, M. Sreejaya et al., ―Biorecognition elements appendedgoldnanoparticlebiosensorsforthedetectionoffood-borne pathogens-a review,‖ Food Control, p. 109510, 2022.

[12] L. Xu, X. Bai, S.Tenguria,Y. Liu, R. Drolia, andA. K. Bhunia, ―Mammaliancell-basedimmunoassayfordetectionofviablebacterial pathogens,‖ Frontiers in Microbiology, vol. 11, p. 575615, 2020.

[13] Y.Jiang,J.Luo,D.Huang,Y.Liu,andD.-d.Li,―Machinelearning advances in microbiology: A review of methods and applications,‖ Frontiers in Microbiology, vol. 13, p. 925454, 2022.