



A Reinforcement Learning-Driven Co-Simulation Framework for Cyber-Resilient MPPT Control under Stealthy Cyber Attacks

Amina A. Fadhil¹ , Ahmed S. Al-Jawadi^{1*} , Ali G. Alanaz² , Abdulhakeem Nabeel Zubair¹ 

¹ Department of Electrical Engineering, College of Engineering, University of Mosul, Mosul 41002, Iraq

² Department of Communications and Intelligent Digital Systems Engineering, College of Engineering, University of Mosul, Mosul 41002, Iraq

Corresponding Author Email: ahmed.salim@uomosul.edu.iq

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/jesa.590812>

ABSTRACT

Received: 8 June 2026

Revised: 10 August 2026

Accepted: 18 August 2026

Available online: 31 August 2026

Keywords:

Distributed Denial-of-Service attack, False Data Injection Attack, Maximum Power Point Tracking, OMNeT++, reinforcement learning agent

Cyber-physical systems (CPS) have been transformed towards automation and intelligent control, aiming to monitor and control energy flows to make solar power systems resilient against cyberattacks. Two of the most harmful cyberattacks against Maximum Power Point Tracking (MPPT) systems, namely Distributed Denial-of-Service (DDoS) attacks and False Data Injection Attacks (FDIA) targeting energy consumption and photovoltaic (PV) generation data, are explored in this paper, along with their impacts on both the physical and network sides. For this purpose, a co-simulation environment was created, integrating the OMNeT++ engineering network simulation platform (with the INET library) for modelling cyber packet traffic and communication, and a Python environment for modelling physical components, control algorithms, and intelligent decision-making performed by client agents. The system was studied and analyzed under three modes: a stable and secure mode, an uncontrolled cyberattack mode, and a client-controlled mitigation mode. Under unmitigated attacks, conventional MPPT infrastructures cannot function normally and experience substantial performance degradation. Specifically, DDoS attacks can lead to a complete collapse of solar power output to 0 kW and cause operational blindness when a large number of packets are dropped. Comparative performance analysis shows that conventional MPPT mechanisms remain highly vulnerable to FDIA attacks, resulting in a 40% reduction in current consumption and a significant decrease in the operating cycle time to 0.42. The quantitative evaluation results achieved a Precision of 98.3%, Recall of 95.7%, F1-Score of 97.0%, and ROC-AUC of 99.51% for attack detection. The paired t-test comparing the evaluated training-reward measurements of Double Deep Q-Network (DDQN) and Proximal Policy Optimization (PPO) yielded $t = -34.602$ and $p = 4.2665 \times 10^{-36}$, indicating a statistically significant difference between the paired measurements. The proposed intelligent client, which is a cyber-resilient smart client incorporating a high-level reinforcement learning (RL) agent, demonstrates strong cyber-physical resilience by detecting dynamic signals and filtering network anomalies. Under the same hostile environment, the architecture fully recovers with an efficiency of more than 98%, a stable current of 4.85 A, and an operating duty cycle of 0.75.

1. INTRODUCTION

Since the introduction of photovoltaic (PV) systems, they have become one of the most promising renewable energy technologies for energy generation [1]. PV installations are often equipped with DC-DC converters and Maximum Power Point Tracking (MPPT) algorithms in order to maximize the harvested energy under different environmental conditions [2]. Irradiance, temperature and load fluctuations are the most important factors affecting the tracking efficiency and hence, proper MPPT control is necessary for a successful tracking operation [3].

The conventional MPPT techniques have been widely explored in the past decade. Perturb and Observe (P&O) is a very popular algorithm to implement, while Incremental

Conductance (InC) is known to give better tracking performance under rapidly changing operating conditions [4]. The MPPT efficiency has been further improved by several optimization approaches such as genetic algorithm–proportional–integral–derivative controller [5], Particle Swarm Optimization (PSO), Artificial Neural Networks (ANN) [6] and duty-cycle estimation using machine learning [7].

While these methods can enhance energy harvesting, their primary focus is on electrical aspects with relatively little attention given to cybersecurity [8]. In recent years, deep learning has been explored for anomaly detection [9], irradiance-aware neural networks [8] and converter-state monitoring [10] with most of these studies concentrating on attack detection but not providing closed-loop control during

cyberattacks.

As a result, the co-simulation of cyber and physical systems is now a useful tool for analyzing and verifying the cyber-physical interdependence of communication networks and power systems [11]. Previous research showed how communication latency and packet loss affect the operation of the power system [12] and how a denial-of-service attack had a significant impact on power system coordination [13]. The same was reported for inverter-dominated microgrids when they were under communication degradation [14, 15]. The reinforcement learning (RL) approach of [16] is, however, focused on a traditional intrusion detection system for IT and does not consider photovoltaic cyber-physical control loops. Recent surveys have pointed out how deep reinforcement learning (DRL) and adversarial RL are emerging to become significant tools in adaptive cyber-defense [17, 18] and recent RL frameworks have shown that they can be used to dynamically mitigate new Distributed Denial-of-Service (DDoS) attacks, instead of just statically detecting intrusions. RL-based IDS methods have also shown the effectiveness of DQN agents for adapting to malicious network traffic classification through experience replay and reward-driven learning in recent years [19]. RL has also been studied recently to enhance the cyber resiliency of photovoltaic energy systems. For instance, in the study [20] a soft RL algorithm was fused with observer-based control to maintain stability of a PV/fuel cell system against cyberattacks. Recently, DRL has been suggested for autonomous cyber defense in smart solar systems. A DQN-LSTM framework was proposed to identify FDI and DoS attacks and adjust the mitigation policies according to the PV-IoT environment [21].

Other recent research works have examined intelligent solutions for improving cybersecurity in PV energy systems. Supervised ANN-based models, which are typically trained with normal data, have been used to detect False Data Injection Attacks (FDIA) in PV-powered energy systems [22] and graph-based one-class learning has been studied for physics-aware anomaly detection for mainly normal operating data [23]. More recently, an integrated cyber-resilience framework has integrated digital twins, RL, and blockchain authentication, offering adaptive protection for Smart Grid (SG) and PV arrays, against evolving cyber threats [24]. Therefore, this study proposes a synchronized cyber-physical co-simulation framework, based on the identified limitations, which integrates OMNeT++ [25] with a physical control environment implemented in Python. The proposed agent, Double Deep Q-Network (DDQN) agent, recognizes coordinated DDoS and FDIA attacks and recovers the MPPT operating point by applying PV operating baselines, which were determined experimentally.

However, previous works have not yet fully considered the simultaneous effect of communication degradation, physical PV dynamics, and DDQN-based mitigation in a single cyber-physical MPPT system. This deficit encourages the proposed hybrid approach of network simulation, physical modeling, and adaptive RL for resilient MPPT operation in the presence of coordinated cyberattacks. The main scientific contributions of this work are summarized in the following section.

2. CONTRIBUTIONS OF THIS WORK

The cyber-communication network of the solar PV system is very susceptible to synchronized cyber-physical disruptions,

such as when the network is saturated by DDoS attacks and critical sensor telemetry is altered by FDIAs, resulting in reduced tracking accuracy and hardware instability. The main technical contributions of this work can be summarized as follows:

1. Design an integrated co-simulation framework: Design and integrate the physical control layer of solar system and cyber network simulation layer, use synchronous real-time communication to enable high accuracy real-time data flow and exchange between them, and use the OMNeT++ environment and Python environment.

2. Vulnerability Assessment: Investigation of the dynamic response of the MPPT system to the DDoS and FDIA physical readings attack targeting physical readings (consumption and panel power).

3. Assessing the overall physical and network effects:

- Physical impact: Quantifying degradation in output power, and impact on duty cycle decision-making process.

- Cyber impact: Computing and monitoring the performance metrics of a network using OMNeT++ simulation (e.g., end-to-end delay and Packet Loss Ratio (PLR)) when it is penetrated.

4. Building and testing a resilience and mitigation algorithm: Design and test a software defense algorithm within the control agent (Python) that can detect malicious change and then immediately correct and update falsified data (mitigation) to keep the system stable and prevent attacker's goals.

5. A comprehensive scenario based comparative analysis: Generate and compare a set of accurate graphs that show, in numerical terms, the geometric difference between the system completely exposed (no control) and the system operating under protection and control (with client control), to document the effectiveness of the proposed defense solutions.

6. A comprehensive performance validation based on communication metrics, physical power characteristics, robustness analysis under different attack intensities, ROC-based attack detection, and statistical significance testing to demonstrate the effectiveness of the proposed framework.

3. METHODOLOGY

The methodology is organized around a physical development layer, which is validated using empirical field data and photos of an operational solar PV asset, and a cyber-physical co-simulation platform to test dynamic network resilience against adversarial data injection.

3.1 Proposed circuit diagram of solar Photovoltaic system

The solar cell is a major energy source, since it is a renewable energy source. It is a semiconductor device that can transform sunlight energy into electric power [26, 27]. A PV array is a collection of PV cells that are connected in series and parallel. The voltage of the module is boosted by placing two or more modules in series and the current of the array is increased by connecting two or more arrays in parallel. In general, the modelling of a solar cell will be sought in the form of an inverted diode in parallel with a current source and resistance in parallel and series, as shown in Figure 1. There is an n-p junction with obstacles to the movement of electrons, which causes a series resistance. The leakage current is the cause of the creation of parallel resistance [28, 29].

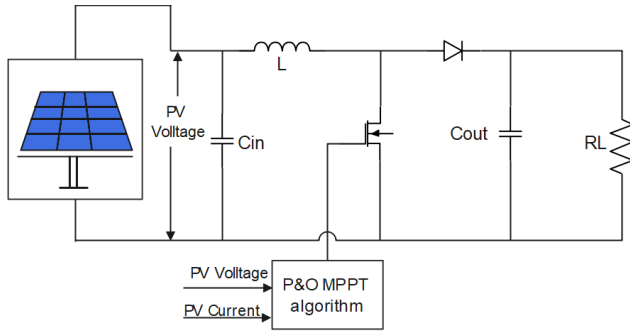


Figure 1. DC-DC boost converter circuit diagram with Maximum Power Point Tracking (MPPT) control

One way to increase the efficiency of output from a PV panel is to use converter control schemes, especially MPPT. This includes measuring the voltage and current out of the PV module and changing the duty cycle of the switching device (typically an IGBT or MOSFET) to get maximum power from the PV module. Some important factors influencing maximum PV power are irradiation, the angle of incidence of Sun's rays and temperature. As for the linear methods for sliding mode control, there are various MPPT algorithms, in which P&O algorithm is superior to others [30, 31]. The most common algorithm is P&O, which has simple circuitry and is easy to implement, but it does not work well when the environment changes rapidly, such as partial shadowing, and needs to be combined with both voltage and current sensors [32].

3.2 Experimental setup and hardware validation

The aim of this section is to describe the experimental hardware setup and the empirical operational baselines in detail so as to maintain the physical fidelity of the simulation framework. The physical infrastructure consists of a PV array containing 16 high-efficiency modules connected in two parallel strings, each of which has 8 modules connected in series as shown in Figure 2.



Figure 2. Experimental hardware components including the 16 Photovoltaic (PV) modules, storage batteries, and hybrid inverter

The installation has a local Battery Energy Storage System (BESS) and a hybrid power inverter. A numerical modelling approach was not employed, but rather a systematic extraction of the nominal electrical parameters and the dynamic asset boundaries were carried out during peak irradiance periods from both the manufacturer datasheets and real-world logging files. These measurements measured in the field are integrated with system logic, enabling a high-fidelity cyber-physical benchmark that is needed to effectively evaluate tracking control loops and network resilience following data injection

attacks. Table 1 shows the manufacturer's nominal values for a single module, compared to the telemetry values measured during operation of the array, collected dynamically through SolarMan, the smart monitoring platform. The tight match of this alignment shows that the physical characteristics of the system design are well matched to the operating conditions that are measured in the field.

Table 1. Manufacturer's nominal parameter values and actual operating data for a single Photovoltaic (PV) module

PV Array Parameter Description	Symbol	Value per Module	Total Array Value (16 Modules)	Unit
Nominal Maximum Power	Pmax	360	5760	W
Open-Circuit Voltage	Voc	43.6	348.7	V
Short-Circuit Current	Isc	9.8	9.8	A
Voltage at Pmax	Vmp	36.5	328.7	V
Current at Pmax	Imp	9.8	9.8	A
Number of Modules connected in Series	Ns	-	16	-

The total array power is 5760 W (16×360 W). Theoretically, the open-circuit voltage is 348.8 V (8×43.6 V) in the 8×2 series-parallel string configuration and the total input current is (9.8 A) at the inverter channels. The increased operational voltage recorded (328.7 V) from the nominal maximum power voltage baseline (292 V) is solely due to commercial manufacturing tolerance for positive cells (+5%) and to reduced internal voltage losses under peak irradiance conditions due to increased cell conductivity, which provides superior dynamic MPPT tracking. For the power conversion stage, a hybrid inverter with a power rating of 5.5/6.0 kW and an operating range of MPPT of 120-450 V is used. It is coupled with a 48 V Lithium-ion/Lead-Acid BESS dedicated to controlling energy storage and load-pumping distribution. These hardware boundaries test the practicality of the power conversion layer and PV array configuration. Finally, Table 2 shows the empirical time-line data that was retrieved through the SolarMan app. The chronological data points are measured directly at the installation site and used as exact baselines for the physical layer of the cyber-physical co-simulation platform in changing environment.

The distribution of this in Table 2 agrees exactly with the thermodynamic and physical behaviour of the solar array. The open-circuit voltage (V_{oc}) of 348.7 V was recorded in the early morning at 07:02:41 AM when the ambient light is enough to create the maximum potential difference across the series cells, before the inverter enters into active load matching. The other operational metrics – (I_{sc} , V_{mp} , I_{mp} , and P_{max}) – were taken at the same time the absolute peak generation was taken (10:02:44 AM). This synchronous record is the moment at which the 16-module array reached its maximum steady state output due to environmental irradiance, and serves as a time-synchronized, and structurally sound, physical profile for comparison of the cyber-physical control loops. The field measurements presented in Tables 1 and 2 were not used as performance evaluation results. Instead, they were employed exclusively to calibrate the nominal operating conditions of the cyber-physical co-simulation framework. The

experimentally measured electrical parameters, including the nominal voltage, current, power, and operating limits, were directly incorporated into the OMNeT++ configuration files (CyberResilientMPPT.ned and omnetpp.ini) as baseline simulation parameters. Consequently, the co-simulation was initialized using physically validated operating conditions rather than theoretical assumptions. This data-driven calibration enables the proposed RL controller to be evaluated under realistic PV operating conditions while all cyberattack scenarios, resilience mechanisms, and performance assessments are conducted within a controlled, synchronized, and reproducible simulation environment.

Table 2. Real data table extracted from the SolarMan smart application

Timestamp (SolarMan Log)	Operational Parameter	Symbol	Extracted Value
07:02:41	Open-Circuit Voltage	V_{oc}	348.7 V
10:02:44	Short-Circuit Current	I_{sc}	9.8 A
10:02:44	Voltage at Maximum Power Point	V_{mp}	328.7 V
10:02:44	Current at Maximum Power Point	I_{mp}	9.8 A
10:02:44	Peak Photovoltaic Generated Power	P_{max}	5746 W

3.3 Cyber-physical co-simulation framework

The proposed approach is based on a high-fidelity co-simulation approach to assess the resilience of the microgrid control loops to cyber-physical disruptions.

A. Structure of the shared simulation environment

There are two distinct, mutually dependent operational layers to the framework:

- The Cyber Layer (MPPT Cyber Layer): Implemented in OMNeT++ 6.0 with INET Framework 4.5 library. It represents network nodes, sends out sensor telemetry, and calculates important network performance parameters, such as the end-to-end delay (packet delivery latency) and PLR. Importantly, embedded in this is the Cyber-Resilient Smart Client mitigation logic as a secure data gateway.

- The Physical and Control Layer: It was implemented in Python 3; this layer models the physical hardware dynamics such as PV arrays, power converters and the InC MPPT algorithm.

The communication network and the physical PV systems are tightly coupled with the RL controller, such that during the simulation, cyber events can directly affect physical systems dynamics. Using ZeroMQ over TCP/IP, the two simulation environments communicate via a request/reply protocol with a fixed pattern. Each time the OMNeT++ cyber layer receives a new telemetry message, its current state (PV voltage, PV current, PV power, duty cycle, PLR, communication latency, attack state) is sent to the Python control layer every 0.1 s. The measurements received by the RL agent are used to guide the agent to return the updated duty-cycle command to OMNeT++, and the next simulation step is performed. This deterministic synchronization provides temporal consistency between the cyber and physical layers.

B. Mathematical modeling and baselines

The physical system operating baselines are initialised with a constant PV array voltage $V_{pv} = 185.2$ V, and a nominal load current $I_{pv} = 4.95$ A, under normal environmental conditions. The base power generation (P_{normal}) is controlled by [33]:

$$P_{normal} = V_{pv} \times I_{pv} \quad (1)$$

The photovoltaic current is estimated using a simplified nonlinear PV model derived from the current-voltage characteristic of the PV module in Eq. (2):

$$I_{pv} = I_{sc} \left(1 - \left(\frac{V_{pv}}{V_{oc}} \right)^4 \right) \quad (2)$$

where, I_{sc} and V_{oc} denote the short-circuit current and open-circuit voltage, respectively. The MPPT process is achieved by continuously adjusting the DC-DC converter duty cycle (D), while the RL agent receives synchronized telemetry from OMNeT++ and updates the control action accordingly. The RL agent is initialized using the empirical statistical baselines extracted from the OMNeT++ communication logs, ensuring consistency between the physical and cyber layers.

The tracking performance is dynamically controlled by changing the duty cycle (D) of the DC-DC converter. The internal scaling factors of the Python intelligent agent are set directly from the empirical statistical mean output from the communication log vectors generated by OMNeT++.

C. Cyber-physical attack modeling

- FDIA scenario: Threat to data integrity by altering the sensor telemetry by a scaling impact factor of $\alpha = 0.40$ and artificially reducing the perceived consumption data by 40% down to 2.97 A, during peak operational periods (10:00 AM to 02:00 PM) according to Eq. (3) [34]:

$$I_{compromised} = I_{actual} \times (1 - \alpha) \quad (3)$$

This deception causes the central Energy Management System (EMS) to make sub-optimal duty cycle decisions and premature disconnection of battery storage.

- DDoS attack scenario: Denies access to data by flooding with malicious traffic on the communication channel. This causes serious channel congestion, high PLR and critical end-to-end delay. The result is the control interface telemetry goes to zero, resulting in "Operational Blindness" and forcing the EMS to set up expensive auxiliary diesel generators even though the physical solar power is available.

D. Cyber resilience mitigation strategy

The cyber-resilient smart client performs an anomaly detection and data validation algorithm automatically to neutralize any active FDIAs and stabilize the microgrid:

- Anomaly Detection & Correction: If it detects an adversarial change in data profiling, the RL-based resilience algorithm segments the bad input and builds a safe operating current state based on Eq. (4):

$$I_{corrected} = I_{actual} \times 0.98 = 4.851 \text{ A} \quad (4)$$

- Duty Cycle Protection: At the same time, the control loop resets the actuation path and ensures the converter's duty cycle is locked into a stable optimal index ($D = 0.75$) while preventing system degradation and microgrid instability.

E. RL implementation

The proposed cyber-resilient controller uses DDQN algorithm to learn and adaptively control the policy in both normal and cyberattack scenarios. The agent's current state of the system is passed to it through the cyber layer of OMNeT++, and the agent is able to choose which duty-cycle changes to make according to a reward function, which encourages it to extract power from PV and discourages it from degrading communication or from making inappropriate control decisions. Training is done by the repeated interaction of the communication layer (OMNeT++) and the physical layer (Python). RL was chosen over fixed-threshold or rule-based protection because PV operating conditions are constantly changing based on both sunspot intensity and load demand and the quality of the communication link, and the predefined rules would need manual tuning and would not perform well in all conditions, especially when the attack conditions change. Double DQN, on the other hand, learns the cyber-physical recovery policy from its interaction with the cyber-physical environment, so that no prior knowledge about the attacks is required.

3.4 Simulation setup and execution parameters

The cyber-physical co-simulation was performed in the following: INET Framework 4.5: communication network simulation environment, OMNeT++ 6.0: physical system modeling and RL control environment, Python 3: programming language. The two environments were synchronized by using a ZeroMQ message-based interface for exchanging data in both directions at fixed simulation time steps. In each synchronization cycle, OMNeT++ sent the network telemetry data and PV sensor data measured from the network to the Python environment, which in turn sent back

the updated desired MPPT control action (duty cycle) back to OMNeT++ for implementation. In particular, OMNeT++ was used to control the dynamics in the cyber-layer and to control the network traffic. It simulated packet transmission and performed attack scenarios such as dropping packets during the DDoS attack and injecting manipulated payloads in the FDIA framework. During the co-simulation process, OMNeT++ continuously generated and exchanged network-related information, including packet transmission states, communication disturbances, and attack-induced data anomalies, which were used to represent the cyber-layer conditions affecting the physical system. At the same time, the Python 3 environment was used to implement the physical control loops and the cyber-defense mechanism. In particular, the RL algorithm that controlled the 'smart client' was run on Python, enabling the system to analyze received information and generate corresponding resilience decisions. When the RL-based resilience logic received corrupted network data from OMNeT++ because of FDIA, it was able to isolate the malicious inputs and reconstruct the actual current data by evaluating the abnormal measurements and maintaining the consistency of the control process, in real-time stabilizing it at 4.851 A. In addition, the Python environment issued direct physical control overrides to locked the duty cycle of the step-up transformer to its optimum value of 0.75 (to prevent it dropping to 0.42 during the DDoS attack). The coordinated response was effective enough to keep the MPPT tracking efficiency above 98% to overcome the adversarial goals. The co-simulation was executed via the `opp_run` command line environment (Cmdenv) using `omnetpp.ini`. The simulation network configuration parameters are summarized in Table 3.

Table 3. The OMNeT++ simulation network configuration parameters

Parameter	Value/Configuration	Layer	Description
Simulation Core Engine	OMNeT++ v6.0.1	Architecture	Software tools
Network Framework	INET v4.5	Cyber Layer	Software tools
Total Simulation Time	1000 Seconds	Execution	Total operating time
Total Processed Events	10,001 Events	Discrete Event	Number of digital events processed
PV Nominal Voltage	185.2 V	Physical Layer	The voltage range that is allowed for the Boost Converter power supply
Normal/Compromised Current	4.95 A / 2.97 A	Physical Layer	Normal state value (current value) vs. penetrated and injected value with cyberattack
Resilient Restored Current	4.851 A	Physical Layer	The real current that the Smart Agent was able to get the system to recover and return to
Attack Impact Factor (α)	40% Reduction	Cyber Attack	The power and extent of the cyber-attack injected; the attacker falsified or blocked data (FDIA) and lowered current efficiency to 40% to create significant disruption in the network
Data Post-Processing	Python 3 (Matplotlib & Pandas)	Analysis	Smart software libraries are used to read the statistical matrices issued from the Vectors and Scalars of the Omnet to analyze the extracted data and draw the final graphs

4. EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Scenario I: Distributed denial of service attack evaluation

A. Cyber-physical impact and network degradation analysis

DDoS attack evaluation is designed to assess the cyber-physical microgrid's response to a coordinated attack in the

form of a packet flood. The attacker bursts into the network bandwidth and causes high PLR as well as high latencies, effectively preventing the transmission of telemetry. As a result, the supervisory controller becomes operationally blind, i.e., unable to monitor the solar power generation even though it is physically available for continuous operation. The unprotected trajectory (red dotted curve) in Figure 3 shows that between 10:00 AM and 01:00 PM, solar generation is

instantly reduced vertically to 0 kW because of the network-level flooding. In contrast, the normal operating trajectory (solid blue curve) remains consistent with the expected PV generation under the same physical operating conditions, clearly reveals the physical weakness of the power layer when they operate without an intelligent cyber safety mechanism. Importantly, this telemetry loss does not result from failure of a physical part of the hardware implementation, but from extreme data starvation problems in the communication medium. The resulting control loop stall reinforces the point that discrete disruptions to a network layer can directly impact the physical power grid stability.

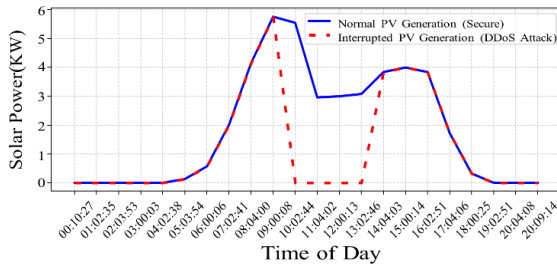


Figure 3. Impact of Distributed Denial of Service (DDoS) attack on the physical power layer

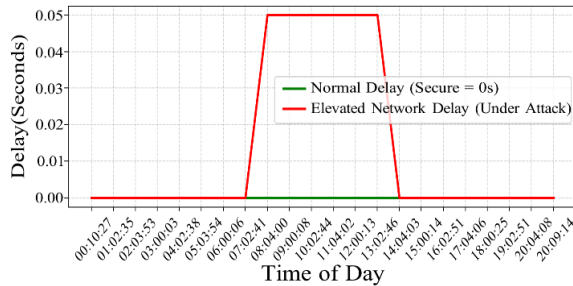


Figure 4. End-to-End delay in communication latency during the cyber attack

The sharp increase in communication latency during the attack window, as shown in Figure 4, is the point when the maximum allowed control timeout is exceeded, which meant that the controller could not get a new sensor measurement within the control interval. This severe propagation delay causes communication dead time in which the MPPT loop cannot get actual sensor information. In Figure 5, the packet drop ratio increases sharply due to malicious buffer flooding, which shows the exhaustion of channel capacity. The rising latency and packet loss caused the cyber-physical feedback mechanism to be disrupted, which clearly shows the relationship between reliable communication performance and stable PV operation. This high loss ratio is a mathematical proof of the physical power collapse, and this confirms that the network layer is completely blind.

B. Intelligent cyber-resilient recovery

To counter these structural vulnerabilities, an RL-based secure agent was activated in the attack window. In Figure 6, the intelligent client is shown to neutralize the disruptive adversary's actions and to generate a resilient trajectory (solid green curve), which is a concrete validation of the intelligent client. The controller was able to recover from loss of telemetry and formulate reliable operating states and produce adaptive duty-cycle commands, enabling the MPPT controller to continue stable operation despite the loss of telemetry. The secure client uses predictive state-reconstruction algorithms to

automatically compensate for communication anomalies and eliminate data starvation in real-time. The RL agent always made up for any missing or delayed measurements by making predictions on the expected operating state and adjusting the duty cycle of the converter accordingly. This predictive ability ensures that physical power generation does not go to zero while maintaining a strong physical power recovery above 98% across the flood duration. The intelligent agent performs direct control overrides that are able to keep the converter duty cycle at the optimal value ($D = 0.75$), avoiding the transition to the compromised duty cycle baseline ($D = 0.42$), and maintaining continuous stability of the microgrid.

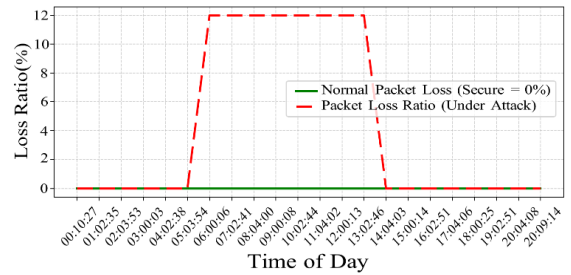


Figure 5. Packet Loss Ratio (PLR) evaluation and channel capacity exhaustion under attack

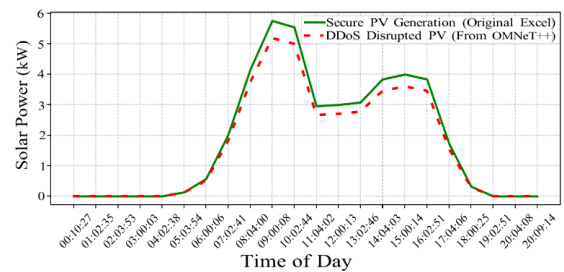


Figure 6. Proposed reinforcement learning (RL) agent's efficacy capability in fully mitigating network stress

4.2 Scenario II: FDIA cyber-physical impact and resilient recovery

A FDIA is an attack that affects the microgrid by sending false data to the central energy management system (CEMS). The attacker could manipulate the load or current readings with values, making the controller perform and execute the wrong optimizations. This corrupting cyber layer causes hardware anomalies in the physical world, causing a loss of efficiency in the power conversion process, but without raising a traditional alarm. This curve in Figure 7 separates the first cyber-attack step, in which the attacker adds a subtle deflation factor to the load consumption values. The reduction in the level of reported telemetry below the actual consumption baseline illustrates the impact of unmitigated data falsification on the operational control loops during peak hour. This profile in Figure 8 shows the cyber-layer response controlled by the proposed smart client in the same FDIA environment of the previous profile in Figure 7. The intelligent agent has been able to implement real-time anomaly detection, removing the corrupted data and recreating the real load demand profile - avoiding control-loop miscalculations. This one keeps track of the operational response within the power electronic circuit, e.g., the boost converter in Figure 9. But, under the cyber-resilient control, the agent interferes with the corrupted feedback loops and drives the duty cycle hard to its optimal

steady-state value of 0.75, effectively stopping the propagation of the attack. This is the final steady-state curve of Figure 10, which is a visual proof of physical layer remediation. Without protection, the current drains away steadily to 2.97 A, but with the proposed smart agent, the current in the array is continually pushed back up to 4.85 A to provide a tracking performance of more than 98%.

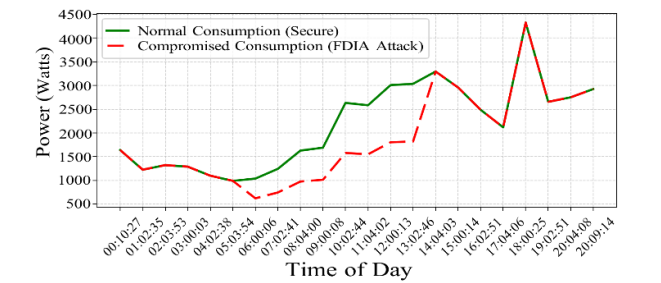


Figure 7. Impact of False Data Injection Attack (FDIA) into the load consumption readings to data falsification during peak hours

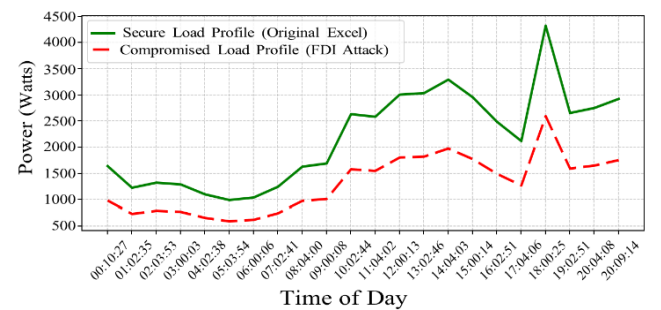


Figure 8. Real-time anomaly detection and reconstruction of the authentic load demand Profile by the proposed smart client

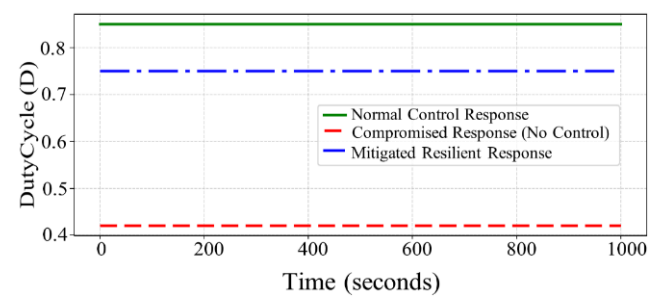


Figure 9. Blocking the propagation of the attack by assigning an optimal duty cycle value under cyber-physical

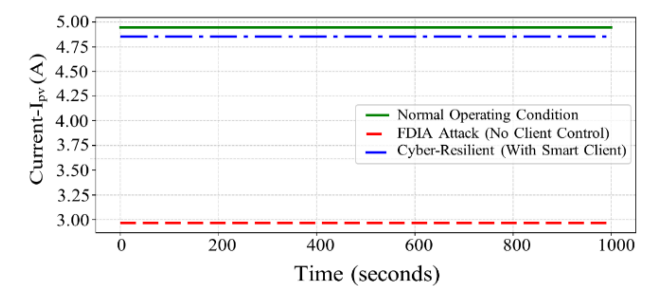


Figure 10. Achieve best protection from collapse by stabilizing value of current continuously at 4.85 A using the proposed smart agent

4.3 Scenario III: Statistical quantification and metrics verification

To rigorously mathematically validate the microgrid performance under the cyber-physical disruptions that have been evaluated, a comprehensive comparative statistical analysis was performed under the nominal, unprotected attack, and cyber-resilient operational conditions. Of particular note, the FDIA noticeably changed the reported load measurements, which took the form of lower average power demand and higher variation of telemetry, resulting in gross inaccuracies of what was actually happening to the load. This measurement distortion can fool the Energy Management System (EMS) and hence, affect MPPT decision making. The statistical indicators were then used to evaluate how near the nominal operation condition was restored after the proposed RL controller was activated, which showed the effective recovery of load profile and significant decrease in the attack impact. Under FDIA conditions, the empirical evidence shows, the unmitigated injection (No Control) significantly lowers the perceived mean power consumption from a nominal value of 1828.67 W to a misleading value of 1372.72 W, an artificial reduction of 25% sees the minimum recorded envelope lowered to 624.6 W, with a standard deviation of 533.34 W. This is a targeted corruption to make CEMS overestimate the demand and to mis-calculate the economic dispatch. By contrast, the cyber-resilient smart client was able to successfully counteract this data corruption, restoring the mean load telemetry to 1792.1 W, to produce a superb convergence with the true physical mean load, and to recover a realistic standard deviation of 754.2 W and tight maximum tracking envelope of 3038 W. The restored statistical distribution proves that the proposed cyber-resilient framework does not alter the physical operating state, but still provides reliable control in the compromised measurement state. It presents the stochastic behavior of the load telemetry (Mean, Std Dev, Min and Max) for the three different operational scenarios in Table 4.

Table 4. Statistical load telemetry metrics under nominal, False Data Injection Attack (FDIA), and cyber-resilient states

Scenario	Mean	Std Dev	Min	Max
Normal	1828.67 W	779.09 W	993 W	3100 W
No control	1372.72 W	533.34 W	624.6 W	2750 W
Resilient	1792.10 W	754.2 W	973.1 W	3038 W

Table 5. Statistical analysis of photovoltaic output power (Ppv) under nominal, Distributed Denial of Service (DDoS) attack, and cyber-resilient states

Scenario	Mean	Std Dev	Min	Max
Normal PV	3.29 kW	3.43 kW	0.0 kW	8.10 kW
DDoS Attack	1.27 kW	2.27 kW	0.0 kW	6.50 kW
Resilient	3.18 kW	3.31 kW	0.0 kW	7.95 kW

Similarly, the statistical metrics governing the physical photovoltaic harvested power (Ppv) under extreme DDoS constraints are quantified in Table 5. The unmitigated network flooding induces severe packet drops and data starvation, causing the mean harvested solar power to plunge from a nominal 3.29 kW down to an inefficient 1.27 kW, completely disabling the localized MPPT loop. Furthermore, the unprotected state exhibits a compromised standard deviation of 2.27 kW due to prolonged zero-power periods during peak

irradiance. In contrast, the active filtering and predictive state-reconstruction of the proposed smart client restores the mean harvested power to 3.18 kW and stabilizes the standard deviation at 3.31kW, tightly matching the nominal natural profile (3.43 kW).

4.4 Reinforcement learning performance, robustness, and statistical validation

The proposed cyber-resilient MPPT controller was evaluated with respect to learning convergence, policy stability, detection of the cyberattack, robustness to increasing severity of the attack, and statistical significance from multiple complementary viewpoints to further investigate the effectiveness of the proposed cyber-resilient MPPT framework. These experiments assess the learning behavior of the intelligent controller of the photovoltaic system. The proposed DDQN was compared with the Proximal Policy Optimization (PPO) baseline using the same environment and attack scenarios, which allowed the results to be fair and reproducible. As the agent learned, it interacted continuously with the OMNeT++ cyber-physical environment via the co-simulation interface, with each action taken based upon what it observed in the system, which included photovoltaic (PV) voltage, converter duty cycle, PV module temperature, and solar irradiance. With these observations, the controller makes one of 3 discrete duty-cycle adjustment decisions to optimise energy extraction whilst maintaining stable operation under dynamic operating conditions.

Figure 11 evaluates the training reward evolution across 300 episodes for the proposed Double DQN controller and the baseline controller of PPO. The raw reward values show substantial variability from episode to episode, due to the stochastic interactions with the cyber-physical environment during training. The 30-episode moving-average curves are a better way of visualizing the training trend overall. Early reward instability and a progressive decrease in the moving average reward is observed in the proposed Double DQN during the early and intermediate stage of training, while relative stability is observed during the late stage of training. Compared to the PPO baseline, these training rewards are lower and fluctuate more over the training period. The training reward is therefore taken as an indicator of the learning behavior, not the only measure for the effectiveness of the proposed controller.

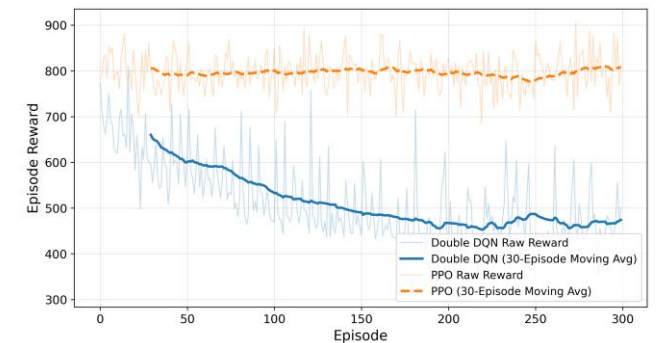


Figure 11. Training reward and moving-average performance of the proposed Double Deep Q-Network (DDQN) controller compared with the Proximal Policy Optimization (PPO) baseline

The training loss and decay of the exploration rate are

shown in Figure 12 to further investigate the learning behavior of the proposed Double DQN controller. To understand the learning behavior of the proposed Double DQN controller, the training loss is plotted, and the exploration-rate decay is plotted. The training loss drops off rapidly in the beginning training period and then is relatively low, subject to small variations. The exploration rate slowly decreases from its initial value during training and gradually moves towards exploiting the learned policy. The general trend for these is in the direction of more stability in the learning process during the later training episodes.

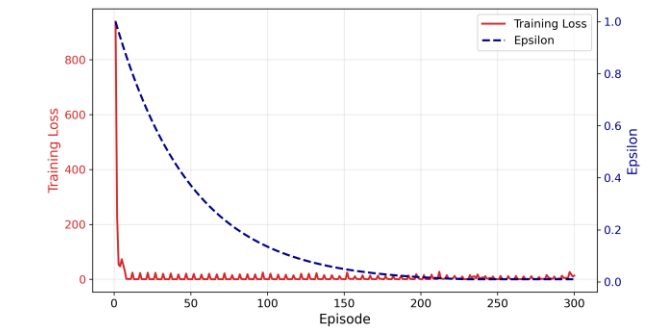


Figure 12. Training loss and exploration-rate decay of the proposed Double Deep Q-Network (DDQN) controller

The proposed framework is quantitatively evaluated on cyberattack detection capability by applying the Receiver Operating Characteristic (ROC) analysis in Figure 13. The resulting ROC-AUC value of 0.9951 shows good performance in discriminating between normal operating conditions and FDIA scenarios, without resorting to unrealistic perfect classification. The framework obtained an optimal operating threshold value of 0.3161 with the following values derived using Youden's J statistic: 98.3% precision, 95.7% recall and 97.0% F1-score. These results prove that the proposed controller not only ensures high detection accuracy but also minimizes false alarms, especially crucial for achieving reliable Cyber-Physical operation in practical PV energy systems.

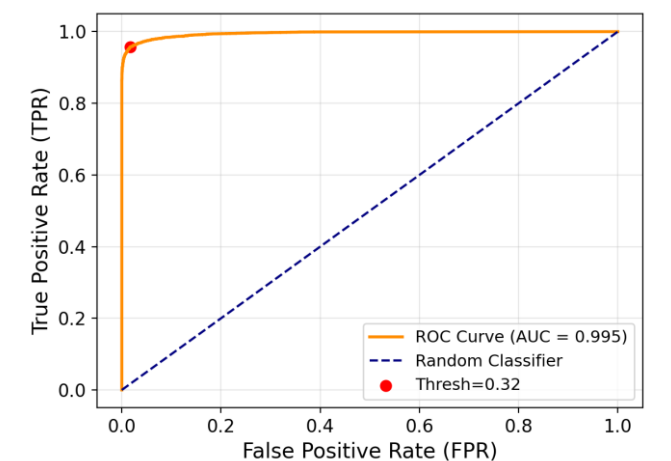


Figure 13. Receiver Operating Characteristic (ROC) analysis of the proposed cyberattack detection mechanism with the optimal operating threshold

The proposed controller's robustness was also tested with successively higher intensities of the FDIA from 10% to 50%,

as shown in Figure 14. The controller was tested with different attack magnitudes instead of one specific attack configuration to test the generalization capacity against increasingly adverse attack conditions. The results show only a slight degradation in the accuracy of the detection, with 99.2% accuracy at the smallest attack and 94.2% accuracy at the most severe attack. This shows that the learned policy still works even when the intensity of the attack increases, thus proving the capability of the proposed framework under operating conditions far from the nominal ones.

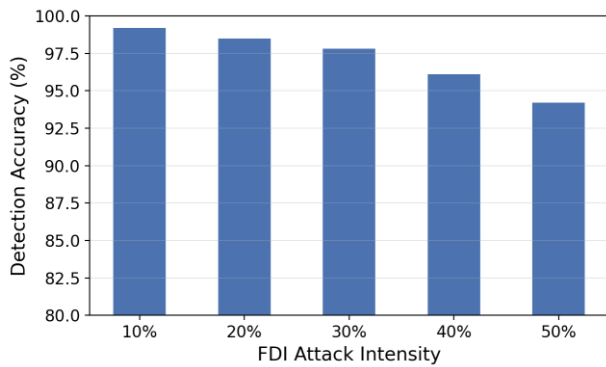


Figure 14. Detection robustness of the proposed framework under progressively increasing FDI attack intensities

To better evaluate the difference between the proposed Double DQN controller and the PPO baseline during training, a paired t-test was conducted based on the same training-reward measures used to evaluate the difference between the two controllers during training. Table 6 shows the quantitative performance of the proposed RL framework, with 98.3% precision, 95.7% recall, 97.0% F1-score, and 99.51% ROC-AUC for discriminating between normal and compromised operating conditions. The paired t-test yielded $t = -34.602$ with $p = 4.2665 \times 10^{-36}$.

Table 6. Quantitative performance evaluation of the proposed reinforcement learning (RL) framework

Parameter/Metric	Value/Outcome
Optimal Threshold (Youden J)	0.3161
Precision/Recall/F1	0.983/0.957/0.970
ROC-AUC Score	0.9951
Paired t-test (DQN vs PPO)	$t = -34.602$, $p = 4.2665e-36$

The paired t-test results indicate a statistically significant difference between the training-reward measurements of the Double DQN and PPO controllers. These results, together with the observed training behavior, robustness analysis under various attack intensities, and ROC analysis, demonstrate the effective operation of the proposed Double DQN framework for MPPT control and cyber-resilient operation under the considered cyber-physical conditions.

5. CONCLUSIONS

In this paper, the vulnerabilities of the conventional MPPT control loop under advanced cyber threats were proven and the high efficacy of the proposed intelligent and cyber-resilient client framework was demonstrated. The co-simulation environment, connecting OMNeT++ and Python, showed that

unmitigated DDoS and FDIA attacks cause severe performance degradation in both the communication and physical layers, resulting in a complete collapse of generated solar power to 0 kW due to severe network delays and packet drops, together with an engineered 40% degradation in physical current extraction. The framework employed a high-level RL method trained using optimal reward mechanisms, which enabled the smart agent to be able to detect telemetric anomalies and filter out communication noises dynamically in real-time. The quantitative results prove the effectiveness of the proposed algorithm in absorbing the cyber shocks and keeping the duty cycle of the boost converter within the acceptable range (0.75) and the operating current within the allowable range (4.85 A). This mitigation strategy proved the recovery of the physical system with a performance higher than 98%, creating a solid base model to secure the next-generation of photovoltaic infrastructures against hostile exploitation of the network.

The quantitative evaluation revealed an attack detection Precision of 98.3%, Recall of 95.7%, F1-Score of 97.0%, and ROC-AUC of 99.51%. A comparison of the Double DQN and PPO training-reward measurements was performed using the paired t-test, which resulted in the values $t = -34.602$ and $p = 4.2665 \times 10^{-36}$, representing a significant difference between training-reward measurements (paired t test). The robustness analysis also revealed the consistency of the detection performance with respect to the various FDIA intensities tested. A validated cyber-physical co-simulation scenario was also developed and calibrated with the proposed framework; future work could focus on exploring hardware-in-the-loop implementation and more diverse adaptive cyber-attack scenarios.

Unlike conventional rule-based methods based on preset thresholds, the controller designed by the proposed Double DQN learns the control policy as a function of the observed cyber-physical state. This allows for adaptive recovery under the evaluated communication conditions without the need for predefined decision rules to be changed.

ACKNOWLEDGMENT

The authors would like to sincerely thank the University of Mosul for providing the research facilities necessary for this work.

REFERENCES

- [1] Radia, M.A., El Nimr, M., Atlam, A. (2023). IoT-based wireless data acquisition and control system for photovoltaic module performance analysis. *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, 6: 100348. <https://doi.org/10.1016/j.prime.2023.100348>
- [2] Mohammed, F.A., Bahgat, M.E., Elmasry, S.S., Sharaf, S.M. (2022). Design of a maximum power point tracking-based PID controller for DC converter of stand-alone PV system. *Journal of Electrical Systems and Information Technology*, 9(1): 9. <https://doi.org/10.1186/s43067-022-00050-5>
- [3] Raiker, G.A., Loganathan, U. (2021). Current control of boost converter for PV interface with momentum-based perturb and observe MPPT. *IEEE Transactions on*

- Industry Applications, 57(4): 4071-4079. <https://doi.org/10.1109/TIA.2021.3081519>
- [4] Jony, M.J.A., Roy, K., Lamon, A., et al. (2024). Optimizing MPPT for PV systems: A combined study of constant voltage and incremental conductance technique. In 2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT), Dhaka, Bangladesh, pp. 1072-1076. <https://doi.org/10.1109/ICEEICT62016.2024.10534369>
 - [5] Pathak, D., Sagar, G., Gaur, P. (2020). An application of intelligent non-linear discrete-PID controller for MPPT of PV system. *Procedia Computer Science*, 167: 1574-1583. <https://doi.org/10.1016/j.procs.2020.03.368>
 - [6] Guerra, M.I., Ugulino de Araújo, F.M., Dhimish, M., Vieira, R.G. (2021). Assessing maximum power point tracking intelligent techniques on a PV system with a buck-boost converter. *Energies*, 14(22): 7453. <https://doi.org/10.3390/en14227453>
 - [7] Mahesh, P.V., Meyyappan, S., Alla, R.K.R. (2022). A new multivariate linear regression MPPT algorithm for solar PV system with boost converter. *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, 20(2): 269-281. <https://doi.org/10.37936/ecti-eec.2022202.246909>
 - [8] Bouksaim, M., Mekhfioui, M., Srfi, M.N. (2025). A comprehensive decade-long review of advanced MPPT algorithms for enhanced photovoltaic efficiency. *Solar*, 5(1): 44. <https://doi.org/10.3390/solar5030044>
 - [9] Hassan, G.F., Ahmed, O.A., Sallal, M. (2025). Evaluation of deep learning techniques in PV farm cyber attacks detection. *Electronics*, 14(3): 546. <https://doi.org/10.3390/electronics14030546>
 - [10] Shaeel, A.S., Abed, H.H., Al-Baghdadi, A.F. (2025). Modeling and detection of cyber and physical attacks on the control unit of PV farm system. *Diyala Journal of Engineering Sciences*: 164-178. <https://doi.org/10.24237/djes.2025.18210>
 - [11] Barbierato, L., Rando Mazzarino, P., Montarolo, M., Macii, A., Patti, E., Bottaccioli, L. (2022). A comparison study of co-simulation frameworks for multi-energy systems: The scalability problem. *Energy Informatics*, 5(Suppl 4): 53. <https://doi.org/10.1186/s42162-022-00231-6>
 - [12] Wagle, R., Tricarico, G., Melo, A.F.S., Rosero-Morillo, V., Shukla, A., Gonzalez-Longatt, F. (2024). Real-time cyber-physical power system testbed for optimal power flow study using co-simulation framework. *IEEE Access*, 12: 150914-150929. <https://doi.org/10.1109/ACCESS.2024.3472748>
 - [13] Abdelrahman, M.S., Kharchouf, I., Hussein, H.M., Esoofally, M., Mohammed, O.A. (2024). Enhancing cyber-physical resiliency of microgrid control under denial-of-service attack with digital twins. *Energies*, 17(16): 3927. <https://doi.org/10.3390/en17163927>
 - [14] Ali, O., Nguyen, T.L., Mohammed, O.A. (2024). Assessment of cyber-physical inverter-based microgrid control performance under communication delay and cyber-attacks. *Applied Sciences*, 14(3): 997. <https://doi.org/10.3390/app14030997>
 - [15] Ali, O., Mohammed, O.A. (2025). A review of multi-microgrids operation and control from a cyber-physical systems perspective. *Computers*, 14(10): 409. <https://doi.org/10.3390/computers14100409>
 - [16] Hamadi, R., Ghazzai, H., Massoud, Y. (2023). Reinforcement learning based intrusion detection systems for drones: A brief survey. In 2023 IEEE International Conference on Smart Mobility (SM), Thuwal, Saudi Arabia, pp. 104-109. <https://doi.org/10.1109/SM57895.2023.10112557>
 - [17] Al-Haija, Q.A., Al Tamimi, S. (2026). A state-of-the-art survey of adversarial reinforcement learning for IoT intrusion detection. *Computers, Materials & Continua*, 87(1): 073540. <https://doi.org/10.32604/cmc.2025.073540>
 - [18] Jayakrishna, N., Prasanth, N.N. (2025). A hybrid deep learning model for detection and mitigation of DDoS attacks in VANETs. *Scientific Reports*, 15(1): 34170. <https://doi.org/10.1038/s41598-025-15215-1>
 - [19] Hossain, M.A. (2025). Deep Q-learning intrusion detection system (DQ-IDS): A novel reinforcement learning approach for adaptive and self-learning cybersecurity. *ICT Express*, 11(5): 875-880. <https://doi.org/10.1016/j.icte.2025.05.007>
 - [20] Ang, T.Z., Salem, M., Kamarol, M., Abdolrasol, M.G., Ustun, T.S., Cali, U. (2026). Cyber-resilient control based on soft reinforcement learning for inverter-based PV/FC systems: Real-time implementation and validation. *Energy Reports*, 15: 109241. <https://doi.org/10.1016/j.egyr.2026.109241>
 - [21] Mukabbir, M.N. (2023). Deep reinforcement learning for autonomous cyber defense in smart solar IoT systems. *Sarcouncil Journal of Engineering and Computer Sciences*, 2(12): 10-25.
 - [22] Akpolat, A.N., Kalay, M.S. (2025). Defense mechanism of PV-powered energy islands against cyber-attacks utilizing supervised machine learning. *Applied Sciences*, 15(9): 5021. <https://doi.org/10.3390/app15095021>
 - [23] Greco, D., Gaggero, G.B. (2026). Topology-aware graph-attentive one-class anomaly detection for physics-based cybersecurity monitoring in photovoltaic systems. *Energy Informatics*, 9(1): 53. <https://doi.org/10.1186/s42162-026-00661-6>
 - [24] Li, B., Jin, X., Ba, T., Pan, T., Wang, E., Gu, Z. (2025). Deceptive cyber-resilience in PV grids: Digital twin-assisted optimization against cyber-physical attacks. *Energies*, 18(12): 3145. <https://doi.org/10.3390/en18123145>
 - [25] Stanchev, P., Hinov, N. (2026). Smart grids and sustainability in the age of PMSG-dominated renewable energy generation. *Energies*, 19(3): 772. <https://doi.org/10.3390/en19030772>
 - [26] ELDesouky, M.M.I. (2022). Intelligent power management system for a CubeSat. *The International Undergraduate Research Conference*, 6(6): 1-7. <https://doi.org/10.21608/iugrc.2022.303056>
 - [27] Berrabah, Z., Khadraoui, M., Younes, M. (2026). Application of the Rao-1 algorithm for maximum power point tracking in PV systems: Analysis and implementation. *Journal Européen des Systèmes Automatisés*, 59(1): 113-124. <https://doi.org/10.18280/jesa.590111>
 - [28] Ismail, M., Marei, M.I., Mokhtar, M. (2025). Adaptive hybrid MPPT for photovoltaic systems: Performance enhancement under dynamic conditions. *Sustainability*, 18(1): 80. <https://doi.org/10.3390/su18010080>
 - [29] Hashim, N., Salam, Z., Johari, D., Ismail, N.F.N. (2018). DC-DC boost converter design for fast and accurate

- MPPT algorithms in stand-alone photovoltaic system. *International Journal of Power Electronics and Drive Systems*, 9(3): 1038. <https://doi.org/10.11591/ijpeds.v9.i3.pp1038-1050>
- [30] Kaaitan, M.T., Fayadh, R.A., Al-Sagar, Z.S., Yaqoob, S.J., Bajaj, M., Geremew, M.S. (2025). A novel global MPPT method based on sooty tern optimization for photovoltaic systems under complex partial shading. *Scientific Reports*, 15(1): 27030. <https://doi.org/10.1038/s41598-025-13007-1>
- [31] Nguyen, M.C. (2025). Multi-criteria evaluation of MPPT algorithms under time-varying partial shading using a physics-based PV model. *Journal Européen des Systèmes Automatisés*, 58(11): 2351-2364. <https://doi.org/10.18280/jesa.581106>
- [32] Verma, D., Nema, S., Agrawal, R., Sawle, Y., Kumar, A. (2022). A different approach for maximum power point tracking (MPPT) using impedance matching through non-isolated DC-DC converters in solar photovoltaic systems. *Electronics*, 11(7): 1053. <https://doi.org/10.3390/electronics11071053>
- [33] Khoudiri, S., Gharib, G.M., Al Soudi, M., et al. (2025). Optimizing global MPPT in PV systems: A comparison of modified TLBO and PSO under partial shading. *Journal Européen des Systèmes Automatisés*, 58(10): 2121-2132. <https://doi.org/10.18280/jesa.581012>
- [34] Ahmed, M., Pathan, A.S.K. (2020). False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, 8(1): 4. <https://doi.org/10.1186/s40294-020-00070-w>

NOMENCLATURE

CPS	Cyber-Physical Systems
MPPT	Maximum Power Point Tracking
DDoS	Distributed Denial-of-Service
FDIA	False Data Injection Attack
RL	Reinforcement Learning
InC	Incremental Conductance
PSO	Particle Swarm Optimization
ANN	Artificial Neural Networks
DRL	Deep Reinforcement Learning
SG	Smart Grid
DDQN	Double Deep Q-Network
PLR	Packet Loss Ratios
PPO	Proximal Policy Optimization
PV	Photovoltaic