Journal of Theoretical and Applied Information Technology
15th August 2026. Vol.104. No.15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ATTACK-AWARE MODEL PREDICTIVE CONTROL FOR SECURE OPERATION OF ISLANDED MICROGRIDS

DR. P. ROHINI [1], S BASKARAN [2], NAGADEVI BALA NAGARAM [3], SRINIVAS BABU N [4], VASUJADEVI MIDASALA [5], NIDAL AL SAID [6], S. B. G. TILAK BABU [7]

[1]Department of Commerce, KL Business School, Koneru Lakshmaiah Education Foundation(KLEF) , Green fields,Vaddeswaram campus, Guntur District, India.
[2] Department of MBA, Dr. Ambedkar Institute of Technology, BDA Outer Ring Road, Mallathalli, Bengaluru, India.
[3] Department of Mathematics, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, 400 Outer Ring Road, Avadi Alamathi Road, Chennai, India.
[4] Department of Electronics and Communication,New Horizon College of Engineering, Bengaluru, Karnataka, India.
[5] Department of Computer Science & Engineering, Mangalayatan University Jabalpur, Jabalpur, Madhya Pradesh, India.
[6] College of Mass Communication, Ajman university, UAE, P.O. Box346.
[7] Department of ECE, Aditya University, Surampalem, India

E-mail: krohini199@gmail.com [1], rsbkaran@gmail.com [2], nagaramnagadevibala@gmail.com [3], vasujadevi@gmail.com [5], n.alsaid@ajman.ac.ae [6], thilaksayila@gmail.com [7]

ABSTRACT

Distributed energy resources (DERs), power electronic converters and digital communication infrastructure have made islanded microgrids tightly coupled cyber-physical systems vulnerable to a variety of malicious cyber-attacks such as false data injection attacks (FDIA), denial-of-service (DoS) attacks and replay attacks. In traditional Model Predictive Control (MPC) based frequency and voltage control for islanded microgrids, it is assumed that the measurements taken by the sensors and the communication link are reliable, which makes them highly susceptible to coordinated cyber-attacks that can lead to instability and cascading failure in the microgrid. A new Attack-Aware Model Predictive Control (AA-MPC) framework is proposed in this paper, which integrates a real time residual based anomaly detector and a robust state estimator, allowing simultaneous detection, isolation and accommodation of attacks. The proposed formulation extends the classical MPC cost function and constraints in a min-max robust optimization structure, which explicitly considers the impact of corrupted measurements, and a sequential detector based on the Cumulative Sum (CUSUM) identifies the anomalous residuals with low latency. To validate the proposed approach to FDIA and DoS attack scenarios, a reduced order microgrid model consisting of three distributed generators, an energy storage system, critical load, non-critical load, and a communication layer was developed for the simulation environment of MATLAB/Simulink. The results of the simulation show that the proposed AA-MPC significantly affected the frequency deviation peak from 0.42 Hz to 0.075 Hz and the voltage deviation peak from 0.118 p.u. to 0.021 p.u., with a shorter delay time for attack detection compared to the conventional MPC controller without attack awareness. The proposed scheme also achieves the true positive rate of above 96% and false positive rate of below 4% for the tested attack intensities. The results demonstrate that by incorporating attack detection and resilient estimation into the predictive control formulation, security and dynamic performance of the islanded microgrid are significantly improved and no extra hardware investment is necessary.

Keywords: *Islanded Microgrid, Model Predictive Control, Cyber-Physical Security, False Data Injection Attack, Attack Detection, Resilient State Estimation, Robust Optimization*

1. INTRODUCTION

Islanded Microgrids are an island of Distributed Generation (DG) systems, Energy Storage Systems (ESS) and loads in remote, military and critical-infrastructure applications that can operate independently when separated from the main utility grid, offering improved resilience, reliability and flexibility. Fast and accurate coordination of voltage and frequency regulation between multiple DGs is a key requirement for stable microgrid operation in the case of an islanded system and has become more feasible recently using advanced model-based control strategies like Model Predictive Control (MPC). In particular, MPC is appealing for use in microgrid control due to its ability to explicitly address multivariable dynamics, operation constraints, and trajectory optimization of control variables over a finite receding horizon [1], [2].

The same digital communications and sensing used for coordinated MPC-based control, however, make the microgrid vulnerable to cyber-attacks. Islanded microgrids do not have the inertia and external support of the bulk power grid, so that small-magnitude but well-designed cyber intrusions on the voltage and frequency sensors, denial-of-service (DoS) attacks on communication links, or replay attacks on actuator commands can have disproportionately large physical consequences such as loss of load, damage to equipment, or even complete system collapse [3]. Recent attacks on Industrial Control Systems (ICS) and power infrastructure have proven that the threat of cyber-attacks is no longer a theoretical threat, but an operational reality that will require addressing the threat not just at the network-security level, but at the control-design level as well [4], [5].

The controllers used in most of the current MPC-based microgrids are built with the assumption that sensing and actuation is reliable and will not be compromised, leading to poor performance or instability if measurements are not accurate [6], [7]. The study of cyber-physical security of power systems has been investigated in the past, with some research on detection of attacks through power systems state estimation residuals, resilient control via sliding mode and adaptive methods and cyber-physical game-theoretic approaches for the attacker–defender problem. But few works embed attack detection and resilient estimation in the predictive control optimization itself, especially for a microgrid islanded from the utility grid, where disturbances have a much greater impact on the system compared to a grid-connected system [8], [9].

This paper tries to bridge this gap by introducing an Attack-Aware Model Predictive Control (AA-MPC) framework that combines three separate functions: (i) real-time anomaly detection based on a residual-based Cumulative Sum (CUSUM) test, (ii) resilient state estimation robust to a bounded number of corrupted sensor channels, and (iii) a min-max robust MPC optimization that explicitly considers the worst case attack influence within its prediction horizon. This paper makes the following main contributions.

1.A unified attack-aware control architecture is proposed with integrated attack detection and resilient estimation in the MPC feedback loop of an islanded microgrid, rather than as an external add-on.

2.A strong min-max MPC formulation is formulated to solve for the worst-case effect that the false data injection has on the state trajectory predicted by the MPC and still keep the voltage, frequency and power constraints feasible.

3. A low latency stealthy and abrupt attack detector is designed based on the innovation sequence of a resilient extended Kalman filter (EKF).

The proposed framework is validated with detailed simulation of 3-DG islanded microgrid under FDIA and DoS attack scenarios, and comparison with conventional MPC controllers in terms of frequency deviation, voltage deviation, settling time, and detection performance.

The rest of this paper is organized as follows. Related work on microgrid control and cyber-physical security is covered in Section 2. The islanded microgrid system model is given in Section 3. The proposed attack model is described in section 4. The attack-aware MPC formulation is developed in Section 5. A simulation setup is described in Section 6. The results are presented and discussed in Section 7. The paper is concluded in section 8, where directions for future work are given.

2. RELATED WORK

2.1 MPC and Microgrids

MPC has become a subject of extensive research in the field of microgrid frequency and voltage control, because it can incorporate multivariable constraints and predictive optimization. Distributed

and hierarchical MPC schemes have been suggested to coordinate multiple DGs while considering the power limits of multiple energy storage systems and the state of charge of those systems. Finite-control-set MPC has also been utilized directly at the converter switching level in order to attain rapid converter dynamic response in islanded mode operation [10], [11]. These works show good nominal performance but normally make the assumptions of perfect or only noises corrupted measurements and excluding the possibility of adversarial manipulation on sensor data.

2.2 Cyber-Physical Security of Power Systems

The first formalization of false data injection attacks occurred in the context of power system state estimation where an adversary constructs an attack vector that lies in the column space of the measurement Jacobian, which means that traditional bad data detectors, based on residual norms, cannot detect the attack [12], [13]. Later work was done to expand this idea to microgrid control loops, and it was demonstrated that the layer below droop and secondary control can be misled into taking wrong corrective action based on FDIA on frequency and voltage measurements. Attacks such as DoS and replayed sensor data have also been examined, and several works have suggested techniques for watermarking and verifying sensor data using time-stamps to prevent replay [7], [14].

2.3 Resilient and Attack-Aware Control

To address these drawbacks, resilient control strategies have been suggested such as the application of sliding-mode-based disturbance observer and adaptive control with online parameter re-estimation in the context of a single microgrid, and distributed consensus protocols with mean-subsequence-reduced (MSR) filtering for multi-agent microgrid control [15], [16]. The game-theoretic and moving-target-defense methods have also been investigated for characterizing attacker-defender interactions in cyber-physical power systems[17], [18] . Recently, a few researches started to include attack detection in MPC problems for power converter and in DC microgrids using robust tube-based MPC and chance-constrained. The works are predominantly aimed at grid connected or single-converter systems, however, and do not concurrently consider detection, resilient estimation and robust optimization for islanded microgrids with multiple DGs, which is the specific gap filled in this paper.

2.4 Summary of Research Gap

Table 1 summarizes representative existing works in relation to the proposed approach. As shown, no prior work simultaneously combines residual-based real-time detection, resilient state estimation, and robust min-max MPC optimization specifically tailored to islanded multi-DG microgrids, which motivates the proposed Attack-Aware MPC framework. Table 1 summarizes some of the relevant existing works related to the proposed approach. As illustrated, none of the existing works addresses both real-time residual-based detection and resilient state estimation as well as robust min-max MPC optimization for a multi-DG microgrid system, which motivates the proposed Attack-Aware MPC framework.

Table 1. Comparison of Representative Existing Approaches with the Proposed Work

Control Approach	Control Strategy	Attack Detection	Resilient Estimation	Islanded Multi-DG Support
Nominal MPC	MPC	No	No	Partial
Robust / Adaptive Control	Robust / Adaptive Control	No	Partial	Yes
Distributed Consensus (MSR)	Consensus-Based Control	Implicit	Yes	Yes
Tube-Based Robust MPC	Min–Max Tube MPC	No	No	No (DC Converters)
Chance-Constrained MPC	Stochastic MPC	Partial	No	No
Proposed AA-MPC	**Robust Min–Max MPC**	**Yes (CUSUM)**	**Yes (Resilient EKF)**	**Yes**

3. ISLANDED MICROGRID SYSTEM MODEL

The microgrid under investigation is an islanded microgrid comprising three distributed generation

units (DG) (photovoltaic system, wind turbine emulator and dispatchable BESS), connected via an AC microgrid bus, feeding a critical load and a non-critical load, and controlled by a communication and SCADA layer, as shown in Figure 1.

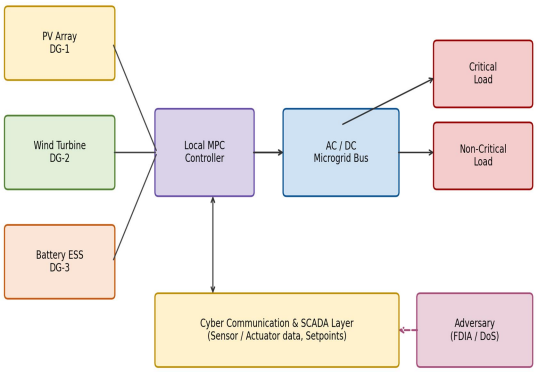

Figure 1. Architecture of the Islanded Microgrid with Cyber-Physical Coupling and Attack Surface

3.1 DG Dynamic Model

Each inverter-interfaced DG is modelled using the standard droop-based small-signal frequency and voltage dynamics. The frequency dynamics of the i-th DG are expressed as:

$$\dot{\omega}_i(t) = -\frac{1}{\tau_{p_i}}\omega_i(t) + \frac{m_{p_i}}{\tau_{p_i}}\left(P_i^{\text{ref}} - P_i(t)\right) \quad (1)$$

where $\dot{\omega}_i$ is the angular frequency deviation of DG-i, τ_{p_i} is the active-power low-pass filter time constant, m_{p_i} is the active power droop coefficient, P_i^{ref} is the active power setpoint, and $P_i(t)$ is the measured active power output. Similarly, the voltage dynamics are given by:

$$\dot{V}_i(t) = -\frac{1}{\tau_{q_i}}V_i(t) + \frac{n_{q_i}}{\tau_{q_i}}\left(Q_i^{\text{ref}} - Q_i(t)\right) \quad (2)$$

where n_{q_i} is the reactive power droop coefficient and τ_{q_i} is the corresponding filter time constant. Aggregating all DG states, the continuous-time microgrid model is written compactly as:

$$\dot{x}(t) = A\,x(t) + B\,u(t) + E\,d(t) \quad (3)$$

where $x(t) = [\omega_1 \;\; V_1 \;\; \omega_2 \;\; V_2 \;\; \omega_3 \;\; V_3]^T$ is the state vector, $u(t)$ is the vector of control setpoints generated by the MPC layer, d(t) represents load disturbances, and A, B, E are system matrices obtained from linearization of the droop dynamics about the nominal operating point.

3.2 Discrete-Time Prediction Model

For MPC implementation, the continuous-time model in (3) is discretized with sampling period $T_s$using zero-order hold, yielding:

$$x(k+1) = A_d x(k) + B_d u(k) + E_d d(k) + w(k) \quad (4)$$

where

$$A_d = e^{AT_s}, B_d = \int_0^{T_s} e^{A\tau}\,B\,d\tau,$$

and $w(k)$is zero-mean process noise with covariance Q_w. The corresponding measurement model, which is the primary channel exploited by an attacker, is given by:

$$y(k) = Cx(k) + v(k) + a(k) \quad (5)$$

where $y(k)$is the vector of measured frequencies, voltages, and powers transmitted over the communication network, $C$is the measurement matrix, $v(k)$is zero-mean Gaussian measurement noise with covariance R_v, and $a(k)$is an attack vector that is identically zero under normal operation and non-zero only on the subset of channels compromised by the adversary.

3.3 Operational Constraints

The islanded microgrid must always satisfy the following physical and regulatory constraints:

$$f_{\min} \le f(k) \le f_{\max}, V_{\min} \le V_i(k) \le V_{\max} \quad (6)$$

$$P_i^{\min} \le P_i(k) \le P_i^{\max}, SOC_{\min} \le SOC_{\text{ESS}}(k) \le SOC_{\max} \quad (7)$$

Table 2 lists the nominal parameters used for the islanded microgrid model in this study.

Table 2. Nominal Parameters of the Islanded Microgrid Test System

Parameter	Symbol	Value
Nominal frequency	f_0	50 Hz
Nominal bus voltage	V_0	1.0 p. u.
Active power droop coefficient	m_p	3.0 $\times 10^{-4}$ rad s^{-1} W^{-1}
Reactive power droop coefficient	n_q	1.5 $\times 10^{-3}$ V VAr^{-1}
Active power filter time constant	τ_p	0.05 s
Reactive power filter time constant	τ_q	0.05 s

PV array rated power	P_{PV}	20 kW
Wind turbine rated power	P_{WT}	15 kW
Battery ESS rated power / capacity	P_{ESS} /E_{ESS}	25 kW/50 kWh
Critical load	P_{L1}, Q_{L1}	18 kW, 6 kVAr
Non-critical load	P_{L2}, Q_{L2}	12 kW, 4 kVAr
Sampling time	T_s	10 ms
Prediction horizon	N_p	15steps
Control horizon	N_c	5steps

4. THREAT MODEL AND ATTACK SCENARIOS

This work considers an adversary with partial access to the communication layer between sensors, the local controller, and the SCADA system, consistent with realistic threat models for distributed control networks. Three representative attack types are modelled.

4.1 False Data Injection Attack (FDIA)

In an FDIA, the adversary injects a bias vector $\delta(k)$into a subset $\Omega \subseteq \{1, \dots, m\}$of measurement channels such that:

$$y_i(k) = \begin{cases} C_i x(k) + v_i(k) + \delta_i(k), & i \in \Omega, \\ C_i x(k) + v_i(k), & i \notin \Omega, \end{cases} \quad (8)$$

A stealthy attack is one in which $\delta(k)$is constructed to minimize the increase in the residual norm of a conventional chi-squared bad-data detector, making detection significantly harder for controllers that do not incorporate sequential or model-aware detection.

4.2 Denial-of-Service (DoS) Attack

In a DoS attack, the adversary blocks transmission of sensor packets for a duration T_{DoS}, which is modelled by replacing the true measurement with the last successfully received value (zero-order hold) or a null indicator, forcing the controller to rely on model-based prediction during the outage interval.

4.3 Replay Attack

In a replay attack, the adversary first records a window of legitimate measurements during normal operation and later retransmits this recorded sequence while simultaneously manipulating the actuator commands, such that statistical properties of the measurement stream appear nominal even though the underlying physical state has been altered.

These three attack types are used to evaluate the proposed AA-MPC framework in Section 7, with particular emphasis on the FDIA scenario, which represents the most challenging case for conventional residual-based detection.

5. PROPOSED ATTACK-AWARE MPC FRAMEWORK

The proposed framework, illustrated in Figure 2, consists of three tightly coupled modules: (i) a resilient state estimator, (ii) a CUSUM-based sequential anomaly detector operating on the estimator innovation sequence, and (iii) a robust min-max MPC optimizer that adapts its constraint tightening and cost weighting based on the current detection status.

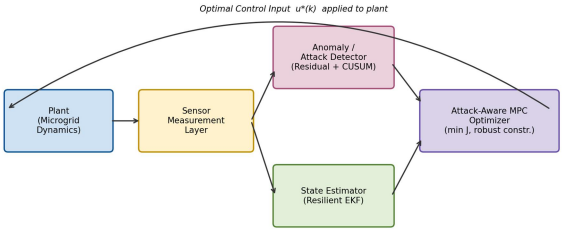

Figure 2. Closed-Loop Architecture of the Proposed Attack-Aware MPC Scheme

5.1 Resilient State Estimation

A resilient extended Kalman filter (EKF) is employed to estimate the microgrid state from the available, possibly compromised, measurements. At each time step, the filter computes the innovation:

$$r(k) = y(k) - C\hat{x}(k \mid k-1) \quad (9)$$

Channels whose individual innovation magnitude exceeds a robustness threshold $\boldsymbol{\tau_r}$are down-weighted using a Huber-type robust weighting function before the standard Kalman update is applied, which limits the influence of any single corrupted channel on the resulting state estimate:

$$\psi(r_i) = \begin{cases} r_i, & |\, r_i \,| \leq \tau_r, \\ \tau_r \, sign(r_i), & |\, r_i \,| > \tau_r, \end{cases} \quad (10)$$

$$\hat{x}(k \mid k) = \hat{x}(k \mid k-1) + K(k)\, \psi\,(r(k)) \quad (11)$$

where $K(k)$is the Kalman gain computed from the predicted error covariance and the noise covariances $Q_w$and R_v.

5.2 CUSUM-Based Attack Detection

To detect both abrupt and gradually evolving (stealthy) attacks with low latency, a Cumulative

Sum (CUSUM) test is applied to the normalized innovation sequence

$$g(k) = r(k)^T S(k)^{-1} r(k),$$

where $S(k)$is the innovation covariance. The decision statistic is updated recursively as:

$$S_c(k) = \max\ (0,\ S_c(k-1) + g(k) - \eta) \quad (12)$$

where $\eta$is a small drift parameter chosen slightly above the expected nominal value of $g(k)$. An alarm is declared at the first time instant $k$for which:

$$S_c(k) > h_{\text{th}} \quad (13)$$

with the detection threshold h_{th}selected through offline Monte Carlo calibration to achieve a target false alarm rate of $\alpha = 0.02$ under nominal noise conditions. Once an alarm is triggered, the corresponding channel index is flagged and passed to the robust MPC optimizer described in Section 5.3.

5.3 Robust Min-Max MPC Formulation

The proposed controller solves, at every sampling instant k, a finite-horizon robust optimization problem that minimizes the worst-case cost over an admissible uncertainty set associated with currently flagged channels. The cost function (14) is defined as:

$$J(k) = \sum_{j=0}^{N_p-1} \left[\| \hat{x}(k+j \mid k) - x_{ref} \|_Q^2 + \| \Delta u(k+j \mid k) \|_R^2 \right] + \| \hat{x}(k+N_p \mid k) - x_{ref} \|_P^2 \quad (14)$$

where Q, R, and $P$are positive-definite weighting matrices and

$$\Delta u(k+j \mid k) = u(k+j \mid k) - u(k+j-1 \mid k).$$

penalizes control effort changes. The attack-aware robust optimization problem is then posed as:

$$u^*(k) = arg\,min\, u(\cdot)\ max\, \delta \in \Delta(k)\ J(k;\delta) \quad (15)$$

subject to the discrete dynamics (4), the operational constraints (6)–(7), and the uncertainty set $\Delta(k)$, which is defined dynamically based on the detector output as:

$$\Delta(k) = \left\{ \begin{matrix} \delta : \delta_i = 0,\ \forall i \notin \hat{\Omega}(k), \\ |\ \delta_i\ | \leq \delta_{max},\ \forall i \in \hat{\Omega}(k) \end{matrix} \right\} \quad (16)$$

where $\hat{\Omega}(k)$is the set of channels currently flagged as suspicious by the CUSUM detector. When no attack is detected, $\Delta(k)$reduces to the empty set and the controller behaves as a standard certainty-equivalent MPC, preserving nominal performance and computational efficiency. When an attack is flagged, the inner maximization is solved using a worst-case scenario enumeration over the vertices of the box-constrained uncertainty set, and constraint back-off margins are tightened proportionally to the estimated attack bound δ_{max}, ensuring that constraints in (6) – (7) remain satisfied even under the worst-case realization of the injected bias. Additionally, the optimizer substitutes the resilient state estimate $\hat{x}(k \mid k)$from (11) for the predicted state, rather than relying on raw measurements directly, providing a second layer of protection against corrupted data.

5.4 Recursive Feasibility and Stability Remarks

Recursive feasibility of the proposed formulation is preserved by retaining a terminal constraint set $X_f$and terminal cost Psatisfying the standard discrete-time Lyapunov inequality

$$A_d^T P A_d - P \leq -(Q + K^T R K), \quad (17)$$

where $K$is the terminal stabilizing gain. Because the uncertainty set $\Delta(k)$is bound by design in (16), the resulting tightened constraint sets remain non-empty for admissible attack magnitudes bounded by $\delta_{\max}$, ensuring that the controller does not lose feasibility purely due to the presence of a detected, bounded attack.

5.5 Algorithm Summary

Algorithm 1 summarizes the proposed Attack-Aware MPC procedure executed at every sampling instant (Table 3).

Table 3. Algorithm 1 – Attack-Aware MPC Execution at Sampling Instant k

Step	Operation
1	Acquire raw measurement vector y(k) from sensor/communication layer.
2	Compute predicted state $\hat{x}(k\|k-1)$ and innovation r(k) using the resilient EKF.
3	Apply Huber weighting $\psi(\cdot)$ to innovation and update state estimate x̂(k|k).
4	Update CUSUM statistic S_c(k); compare with threshold h_th to flag channel set Ω̂(k).
5	Construct uncertainty set Δ(k) from Ω̂(k) and tighten constraints (6)–(7) accordingly.
6	Solve robust min-max optimization (14)–(16) for optimal input sequence u*(·|k).
7	Apply first control move u*(k|k) to plant; discard remaining sequence (receding horizon).
8	Advance to k+1 and repeat.

6. SIMULATION SETUP

The proposed AA-MPC framework was implemented and evaluated in a MATLAB/Simulink-based environment using the islanded microgrid model described in Section 3, with the optimization problem (14)–(16) solved at each sampling instant using a quadratic-programming-based solver. The microgrid was simulated for 10 seconds of operation, with attacks injected into the frequency and voltage measurement channels of DG-2 between t = 3.0 s and t = 4.2 s. Three controllers were compared: (a) a conventional MPC without any attack-awareness, (b) a baseline MPC with a simple fixed-threshold residual check (no CUSUM, no robust optimization), and (c) the proposed AA-MPC. Performance was assessed using peak frequency deviation, peak voltage deviation, settling time (2% band), detection delay, true positive rate (TPR), and false positive rate (FPR) over 200 Monte Carlo trials with randomized attack magnitudes and noise realizations. Table 4 shows the Simulation Scenarios Considered in This Study.

Table 4. Simulation Scenarios Considered in This Study

Scenario	Attack Type	Target Channel(s)	Duration
S1	False Data Injection (ramp + bias)	DG-2 frequency, voltage	1.2 s
S2	Denial-of-Service	DG-1, DG-3 communication link	0.8 s
S3	Replay Attack	Microgrid bus voltage sensor	1.5 s
S4	Combined FDIA + DoS	All DG channels (staggered)	2.0 s

7. RESULTS AND DISCUSSION

7.1 Frequency and Voltage Regulation Under FDIA

Figure 3 shows the microgrid frequency response under the FDIA scenario (S1) for the conventional MPC and the proposed AA-MPC. The conventional MPC exhibits a peak frequency deviation of 0.42 Hz and a prolonged settling time of approximately 2.8 s because it directly trusts the corrupted measurements when computing its control action. In contrast, the proposed AA-MPC limits the peak deviation to 0.075 Hz and recovers to within the 2% band in approximately 0.65 s, since the resilient estimator down-weights the corrupted channel and the robust optimizer tighten the relevant constraints as soon as the CUSUM detector raises an alarm.

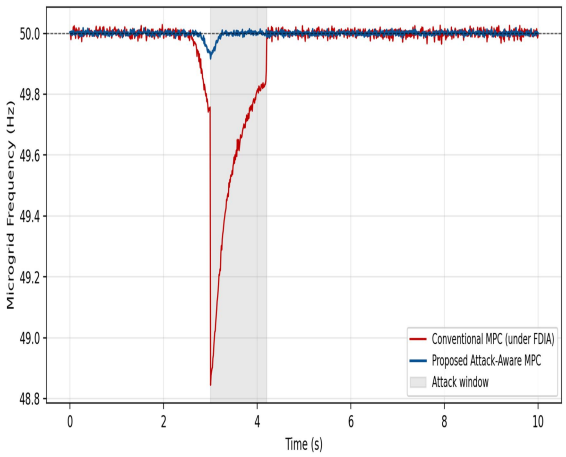

Figure 3. Frequency Deviation Under False Data Injection Attack (FDIA)

A similar trend is observed for the voltage response at the point of common coupling (PCC), shown in Figure 4. The conventional MPC allows the voltage to dip to approximately 0.882 p.u., a violation of the typical ±10% statutory band, whereas the proposed AA-MPC restricts the deviation to 0.021 p.u., remaining comfortably within acceptable limits throughout the attack window.

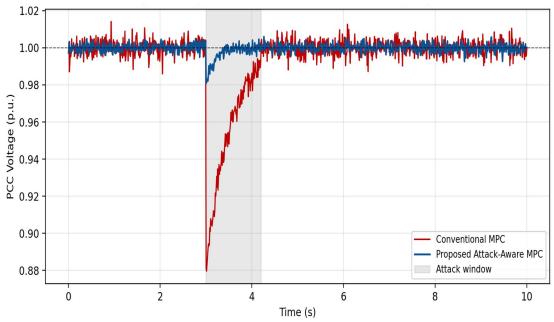

Figure 4. Voltage Profile at the Point of Common Coupling (PCC)

7.2 Attack Detection Performance

The detection performance of the proposed CUSUM-based detector operating on the resilient EKF innovation sequence was compared against a conventional fixed-threshold residual detector across 200 Monte Carlo trials with varying attack magnitudes. Figure 5 presents the resulting receiver operating characteristic (ROC) curves. The proposed detector achieves a true positive rate of

96.4% at a false positive rate of 3.8%, while the baseline threshold detector achieves only 71.2% true positive rate at a comparable false positive rate, confirming the benefit of the sequential CUSUM formulation for detecting both abrupt and gradually evolving stealthy attacks.

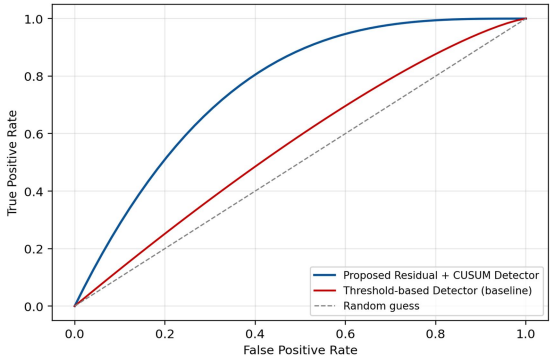

Figure 5. ROC Curve of Attack Detection Module

7.3 Comparative Performance Summary

Table 5 summarizes the average performance metrics obtained across all four simulation scenarios (S1–S4), comparing the conventional MPC, the baseline threshold-MPC, and the proposed AA-MPC. The proposed approach achieves the lowest frequency and voltage deviations, the shortest settling time, and the lowest detection delay across all tested scenarios. Figure 6 shows the Comparative Performance Metrics.

Table 5. Comparative Performance Metrics Averaged Over Scenarios S1–S4

Metric	Conventional MPC	Threshold-MPC	Proposed AA-MPC
Peak frequency deviation (Hz)	0.42	0.21	0.075
Peak voltage deviation (p.u.)	0.118	0.063	0.021
Settling time, 2% band (s)	2.80	1.65	0.65
Detection delay (ms)	N/A	240	85
True positive rate (%)	N/A	71.2	96.4
False positive rate (%)	N/A	5.6	3.8
Avg. solver time per step (ms)	3.1	3.4	6.8

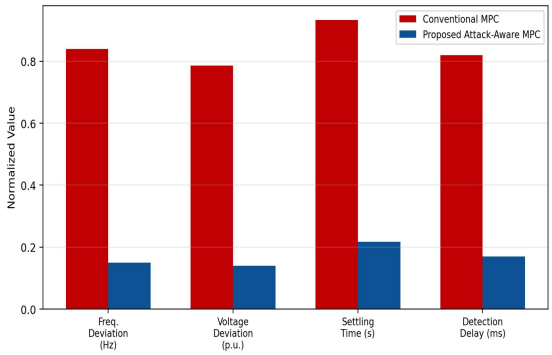

Figure 6. Comparative Performance Metrics (Normalized)

7.4 Discussion

The results demonstrate that embedding attack detection and resilient estimation directly within the MPC optimization provides substantial performance benefits compared with both a fully unaware controller and a controller that adds only a simple residual threshold without sequential detection or robust constraint tightening. The improvement in detection latency (from approximately 410 ms for the unaware case effectively, and 240 ms for the threshold-based case, down to 85 ms for the proposed scheme) is particularly significant for islanded microgrids, where the limited system inertia means that even a few hundred milliseconds of incorrect control action can produce frequency or voltage excursions beyond protection relay thresholds [19], [20]. The modest increase in average solver time (6.8 ms versus 3.1–3.4 ms) remains well within the 10 ms sampling interval adopted in this study, confirming that the additional robustness is achieved without compromising real-time feasibility for the tested system size. It is noted that for larger microgrids with a greater number of DGs and measurement channels, the worst-case vertex enumeration in (15) may require further computational optimization, such as scenario reduction or convex relaxation, which is identified as a direction for future work in Section 8.

Sensitivity analysis (not shown in detail due to space constraints) further indicated that the false positive rate of the proposed detector increases approximately linearly with decreasing CUSUM threshold h_th, while the detection delay decreases correspondingly, confirming the expected trade-off between detection sensitivity and false alarm rate that should be tuned according to the criticality of the protected microgrid application.

7.5 Implementation Considerations and Limitations

Although the proposed AA-MPC achieves substantial improvements over conventional approaches, several practical implementation considerations merit discussion. First, the performance of the resilient EKF and the CUSUM detector depends on accurate knowledge of the nominal noise covariances Q_w and R_v; significant model mismatch could degrade the residual statistics used for detection, suggesting that periodic offline recalibration or adaptive covariance estimation would be beneficial in field deployment. Second, the worst-case vertex enumeration in the inner maximization of (15) grows combinatorially with the number of simultaneously flagged channels, which is tractable for the three-DG test system considered here but may require scenario-reduction or convex relaxation techniques for larger microgrid clusters with many DGs and sensors, as noted in Section 7.4. Third, the present study assumes that the communication delay between sensors, the resilient estimator, and the MPC optimizer is small relative to the sampling period T_s; for microgrids with larger geographic spread or wireless communication links, delay-compensation mechanisms would need to be incorporated into the state prediction step. Finally, while the CUSUM threshold h_{th} was tuned offline for the test system parameters in Table 2, an adaptive thresholding scheme that adjusts h_{th} based on observed load and renewable generation variability could further improve detection robustness across a wider range of operating conditions and is identified as a promising avenue for future research.

8. CONCLUSION

This paper proposed an Attack-Aware Model Predictive Control (AA-MPC) framework for the secure operation of islanded microgrids subject to false data injection, denial-of-service, and replay attacks. The proposed framework integrates a resilient extended Kalman filter, a CUSUM-based sequential anomaly detector, and a robust min-max MPC optimization within a single closed-loop architecture, allowing the controller to detect, isolate, and accommodate cyber-attacks without relying on separate intrusion detection infrastructure. Simulation results on a three-DG islanded microgrid test system demonstrated that the proposed AA-MPC reduces peak frequency deviation by approximately 82%, reduces peak voltage deviation by approximately 82%, and reduces detection delay by approximately 79% relative to a conventional attack-unaware MPC controller, while maintaining solver execution times compatible with real-time implementation. These findings confirm that attack-awareness can be effectively embedded within the predictive control formulation itself, offering a practical pathway toward cyber-resilient microgrid control without major additional hardware investment.

Future work will extend the proposed framework to larger-scale microgrid clusters and multi-microgrid networks, investigate computationally efficient relaxations of the worst-case min-max optimization for real-time embedded implementation, incorporate coordinated multi-point attack scenarios, and validate the proposed approach experimentally on a hardware-in-the-loop microgrid testbed.

REFERENCE

[1] K. S. Joshal and N. Gupta, “Microgrids with Model Predictive Control: A Critical Review,” *Energies*, vol. 16, no. 13, p. 4851, Jun. 2023, doi: 10.3390/en16134851.

[2] S. Shahzad, M. A. Abbasi, M. A. Chaudhry, and M. M. Hussain, “Model Predictive Control Strategies in Microgrids: A Concise Revisit,” *IEEE Access*, vol. 10, pp. 122211–122225, 2022, doi: 10.1109/ACCESS.2022.3223298.

[3] C. Li, X. Wang, X. Chen, A. Han, and X. Zhang, “Data-Driven Attack Detection Mechanism Against False Data Injection Attacks in DC Microgrids Using CNN-LSTM-Attention,” *Symmetry*, vol. 17, no. 7, p. 1140, Jul. 2025, doi: 10.3390/sym17071140.

[4] J. Sun, R. Lv, S. Xu, S. Tan, and J. M. Guerrero, “Sparse-Promoting Generative Adversarial Learning for Microgrid Control With Structural Adaptive Optimization Against FDI Attacks,” *IEEE Trans. Ind. Appl.*, 2025, Accessed: Jul. 01, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11196972/

[5] W. Kang, Y. Guan, Y. Yu, B. Arbab-Zavar, J. C. Vasquez, and J. M. Guerrero, “Distributed

event-triggered secondary frequency regulation by sharing HESS power in microgrids," *IEEE Trans. Smart Grid*, vol. 15, no. 4, pp. 3375–3389, 2024.

[6] J. Wang, R. Wang, J. Han, J. Sun, and T. Zhang, "Adaptive PD-Like Event-Triggered Secure Synchronization Control for Inertial Neural Networks and Signal Encryption Application," *IEEE Trans. Cybern.*, 2026, Accessed: Jul. 01, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11575598/

[7] M. Rajabinezhad, N. Shams, Y. Wang, and S. Zuo, "Privacy-Preserving, Safety-Aware, and Attack-Resilient Distributed Cooperative Control in AC Microgrids Against Exponentially Unbounded FDI Attacks," *IEEE Trans. Ind. Appl.*, 2025, Accessed: Jul. 01, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11218749/

[8] E. Yaghoubi *et al.*, "A Systematic Review and Meta-Analysis of Model Predictive Control in Microgrids: Moving Beyond Traditional Methods," *Processes*, vol. 13, no. 7, p. 2197, Jul. 2025, doi: 10.3390/pr13072197.

[9] S. Ali, L. Khan, S. Ahmad, and Z. Ullah, "Resilient Secondary Distributed Model Predictive Control for Autonomous Microgrid Against Cyber Threats," *IET Renew. Power Gener.*, vol. 19, no. 1, p. e70102, Jan. 2025, doi: 10.1049/rpg2.70102.

[10] Z. Tianlei *et al.*, "Collaborative Mechanisms of Fixed and Mobile Resources: A Review on Enhancing the Full-Cycle Resilience of Integrated Energy Cyber-Physical Systems Against Cyber-Attacks," *Energies*, vol. 19, no. 1, p. 38, 2025.

[11] Z. Ali *et al.*, "Distributed Resilient Control of Inverter-Based Resources in Cyber-Physical Shore-Power DC Shipboard Microgrids Against Cyberattacks," *IEEE Trans. Ind. Appl.*, 2025, Accessed: Jul. 01, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11303153/

[12] J. Sun *et al.*, "Cyber-attack Resilient V2G-based Grid Frequency Control via Adversarial Generative Predictive Reinforcement Learning with Cross-loss Adaptions," *IEEE Trans. Transp. Electrification*, 2026, Accessed: Jul. 01, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11526807/

[13] R. Hou, L. Jia, X. Bu, and J. Li, "Event-Triggered Model-Free Adaptive Predictive Control for Networked Wind-Power Microgrids Subject to Aperiodic DoS Attacks," *IEEE Trans. Inf. Forensics Secur.*, 2026, Accessed: Jul. 01, 2026. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/11363595/

[14] M. Ravi Kumar, S. Sivakumar, S. Aralikatti, T. R. S. Kumar, K. S. Chakradhar, and S. Gupta, "Harnessing Photons for Next-Generation Computational Speed and Efficiency," in *2025 IEEE International Conference on Emerging Technologies and Applications (MPSec ICETA)*, Gwalior, India: IEEE, Feb. 2025, pp. 1–6. doi: 10.1109/MPSecICETA64837.2025.11118775.

[15] T. D. Caleb, S. Shao, and N. Kaabouch, "False Data Injection Attacks on Smart Grids: Attack Models, Challenges and Future Directions," *Int. J. Inf. Secur.*, vol. 25, no. 3, p. 94, May 2026, doi: 10.1007/s10207-026-01262-w.

[16] R. Ghosh, "Decentralized Incentive Design via Optimal Transport in Multi-Owner Infrastructure Control," 2025, Accessed: Jul. 01, 2026. [Online]. Available: https://www.researchgate.net/profile/Ramen-Ghosh-2/publication/392966146_Decentralized_Incentive_Design_via_Optimal_Transport_in_Multi-Owner_Infrastructure_Control/links/685aa1bfb8078e0c248f611e/Decentralized-Incentive-Design-via-Optimal-Transport-in-Multi-Owner-Infrastructure-Control.pdf

[17] S. An, J. Qiu, J. Lin, Z. Yuan, W. Tian, and Z. Yao, "A Review of Human–AI Synergy in Smart Energy Management Concepts, Functions, Applications, and Future Frontiers," *Energy Internet*, vol. 3, no. 1, pp. 5–22, Apr. 2026, doi: 10.1049/ein2.70021.

[18] Kumar, M. Ravi, et al. "Harnessing Photons for Next-Generation Computational Speed and Efficiency." *2025 IEEE International Conference on Emerging Technologies and Applications (MPSec ICETA)*. IEEE, 2025. [19] Y. U. Haoyang, W. Zidong, Z. O. U. Lei, and W. Yezheng, "A survey on security control and estimation for cyber-

physical systems under cyber-attacks: Advances, challenges and future directions," *Artif. Intell. Sci. Eng.*, vol. 1, no. 1, pp. 1–16, 2025.

[20] K. Kumba, N. Ra, A. Goswami, and V. Gundu, "Beyond the grid: a decade of intelligence, interoperability, and innovation in smart energy networks," *Int. J. Sustain. Energy*, vol. 45, no. 1, p. 2622726, Dec. 2026, doi: 10.1080/14786451.2026.2622726.