Scientific Reports

https://doi.org/10.1038/s41598-026-44084-5

Article in Press

Observer aided robust control for cyber physical power grids with event triggered sliding mode controller

Received: 26 September 2025

Accepted: 9 March 2026

Published online: 18 March 2026

Cite this article as: Mohanty A., Ramasamy A., satpathy A. *et al.* Observer aided robust control for cyber physical power grids with event triggered sliding mode controller. *Sci Rep* (2026). https://doi.org/10.1038/s41598-026-44084-5

Asit Mohanty, Agileswari Ramasamy, Abhaya satpathy, S. Mohanty, Reji Kumar Rajamony, Javed Khan Bhutto, Hadi Hakami, P. Mohanty, A. Megalingam & Haiter Lenin Allasi

Observer Aided Robust Control for Cyber Physical Power Grids with Event Triggered sliding mode Controller

Asit Mohanty[1,2], Agileswari Ramasamy[1], Abhaya satpathy[3], S Mohanty[4], Reji Kumar Rajamomny[5,6], Javed Khan Bhutto[7], Hadi Hakami[7], P Mohanty[8], A. Megalingam[9], Haiter Lenin Allasi[10*]

[1]Institute of Power Engineering, UNITEN, Kajang, Kuala Lumpur, Malaysia
[2]Centre for Promotion of Research, Graphic Era(deemed to be university), Clementtown, Dehradun. India.
[3]Faculty of Management studies, Sri Sri University, Cuttack, India
[4]School of Computer Sciences, OUTR, Bhubaneswar, India
[5]Institute of Sustainable Energy, Universiti Tenaga Nasional (The Energy University), Jalan Ikram-Uniten, Kajang 43000, Selangor, Malaysia
[6]Faculty of Engineering and Technology, Parul University, Waghodiya Road, Vadodara – 391760, Gujarat, India
[7]Department of Electrical Engineering, King Khalid University, Abha, Saudi Arabia
[8]Department of Mechanical Engineering, VSSUT, Burla, India
[9]Faculty of Mechanical & Automotive Engineering Technology, University Malaysia Pahang Al-Sultan Abdullah, Pekan 26600, Pahang, Malaysia
[10*]Department of Mechanical Engineering, WOLLO University, Kombolcha Institute of Technology, Ethiopia. Post Box No: 208, Kombolcha

*Corresponding Author email: drahlenin@kiot.edu.et , haiterlenina@gmail.com

Abstract: The growing integration of renewable energy in both islanded and interconnected microgrids has rendered Cyber-physical stability and resilience a vital area of research. Conventional controllers, including PID and linear state-feedback, are susceptible to network-induced delays, denial-of-service (DoS) attacks, and false data injection, resulting in diminished reactive power support and the risk of voltage collapse. This paper proposes an Observer-Aided Robust Control Framework that integrates an Event-Triggered Sliding Mode Controller (ET-SMC) with improved anomaly detection to address these challenges. An Extended Kalman Filter (EKF) and Sliding Mode Observer (SMO) are formulated to estimate hidden state variables and identify malicious data alterations with high sensitivity, facilitating dependable control decisions in the presence of Cyber-attacks. The performance of anti-windup PID and baseline SMC is evaluated against ET-SMC with observer augmentation, demonstrating that the proposed strategy offers enhanced robustness, quicker transient response, and diminished chattering. A stability-guaranteed Event-triggered communication protocol is developed through Lyapunov analysis to reduce bandwidth consumption while maintaining voltage and reactive power regulation. The proposed framework is validated on a real-time OPAL-RT hardware-in-the-loop (HIL) microgrid testbed, demonstrating its effectiveness in scenarios involving renewable intermittency, communication noise, and coordinated Cyber-attacks. Comparative results demonstrate that ROC-based detection performance and time-domain simulations underscore the advantages of observer-aided ET-SMC in ensuring resilient, low-bandwidth, and real-time Cyber-physical control for next-generation power grids.

Key words: Cyber physical power grid, Event trigger control, sliding mode control, Extended kalman filter, Reactive power control, Resiliency

Nomenclature-

Symbol	Description
(A, B, C)	Continuous-time system matrices (state, input, output)
α, β	Positive design scalars
CPS	Cyber-Physical Systems

CPPS	Critical Cyber-Physical Systems
(d(t))	Unknown disturbance or attack signal
$\hat{d}$	Reconstructed disturbance estimate
δ	Bounded disturbance level
DG	Distributed Generation
DDoS	Distributed Denial-of-Service Attack
DoS	Denial-of-Service Attack
DRAs	Data Replay Attacks
EKF	Extended Kalman Filter
ETSMC	Event-Triggered Sliding Mode Control
FACTS	Flexible AC Transmission System
FDI	False Data Injection
FDIA	False Data Injection Attack
FPGA	Field-Programmable Gate Array
(F)	Set of faulty or attacked communication channels
HIL	Hardware-in-the-Loop
HMIs	Human–Machine Interfaces
ICS	Industrial Control Systems
I_d, I_q	d–q axis currents
IG	Induction Generator
ISE	Integral Squared Error
(J)	Lyapunov function or cost function
(K)	EKF Kalman gain
K_s	Sliding mode control gain (discontinuous component)
(L, R)	Inductance and resistance
L_{SMO}	Sliding Mode Observer (SMO) injection/gain matrix
λ_{min}	Minimum eigenvalue of a matrix
(P)	EKF error-covariance matrix
(P, Q)	EKF process and measurement covariance matrices
RES	Renewable Energy System
Γ	Event-trigger threshold parameter
$\Delta = y(t_k - y(t))$	Triggering error
$\hat{x}$	State estimate (observer/EKF/SMO)
$\tilde{x}=x-\hat{x}$	State estimation error
(x)	System state vector
(y)	Measurement/output vector
(u)	Control input vector
u_{eq}	Equivalent (continuous) control component of SMC
ω	Grid angular frequency
σ	Sliding variable(often=s(x,t))
(s(x,t))	Sliding surface function
SG	Synchronous Generator
SMC	Sliding Mode Control
SMO	Sliding Mode Observer
STATCOM	Static Synchronous Compensator
SVC	Static VAR Compensator
T_s	Minimum inter-event time (to prevent Zeno behavior)
TSA	Time Synchronization Attack
t_k	k-th triggering instant
SCADA	Supervisory Control and Data Acquisition
u_{sw}	Switching (discontinuous) control part

$\|*\|$	Euclidean or induced matrix norm
USB	Universal Serial Bus
V_d, V_q	d–q axis voltages
η	Boundary layer or saturation thickness
(0)	Zero vector or zero matrix

1. Introduction

The growing integration of power grids with communication and computing infrastructure has converted traditional electrical networks into Cyber-physical systems (CPS)[1],[2].This incorporation facilitates advanced monitoring, distributed control, and efficient energy management; however, it also introduces vulnerabilities, including Cyberattacks, data integrity issues, and communication delays. False Data Injection (FDI) and Denial-of-Service (DoS) assaults make micro grids and interconnected power systems lesser stable and reliable by interacting with sensor signals or obstructed control signals[3], [4]. Securing resilience against Cyber-physical attacks has emerged as a critical research challenge. Observer-based control systems have arisen as an effective approach to tackle these challenges[5]. Additional observers, such as the Extended Kalman Filter (EKF) and Sliding Mode Observer (SMO), can estimate system states even in the presence of damaged or absent data, thereby enabling resilient failure and attack detection. The incorporation of these estimate frameworks alongside intelligent control mechanisms enhances power grid resilience by isolating anomalies and maintaining stable operation[6], [7]

Sliding Mode Control (SMC) has gained significant recognition for its resilience in managing parameter uncertainty and external disturbances in nonlinear power system dynamics. Also, its implementation in continuous time often has higher communication needs and chattering problems[8]. To get around these problems, Event-triggered sliding mode control techniques have been used. These only send control updates when a certain error threshold is reached. Also, this cuts down on communication overhead and keeps the system stable, making it perfect for smart grid applications with limited bandwidth[9],[10].

Combining observer-based estimation with Event-triggered sliding mode control (SMC) creates a useful framework for improving Cyber resilience in managing voltage and reactive power in multi-area grids and microgrids[11], [12]. This study introduces an observer-assisted Event-triggered sliding mode control system that employs the Extended Kalman Filter (EKF) and Sliding Mode Observer (SMO) for anomaly detection, state reconstruction, and disturbance rejection. The controller has been engineered to improve voltage stability as well as provide reactive power provision during Cyber-physical attacks, communication delays, as well as parameter uncertainties[13]–[15],[16]. Previous research has examined Lyapunov-based methods for realizing triggering conditions which preserve system stability despite uncertainty.Zhang et al. discussed adaptive ETC methods that dynamically improve triggering thresholds based on real-time performance data. Liu et al. similarly discussed how Lyapunov functions may improvise voltage regulation methods to maintain safe operating conditions.Further, reinforcement learning techniques have been utilized to improve triggering tactics through experience-driven adaptation, enabling more robust as well as responsive control.

Recent literature has significantly progressed both event-triggered control and cyber-resilience for power systems in essential yet complementary manners. Guo et al. and Liu et al.[17], [18] provide significant insights into event-triggered sliding-mode and fixed-time consensus strategies for networked nonlinear systems and DC microgrids, respectively, illustrating the attainment of communication efficiency and finite-time convergence despite imperfect sources. Qi et al.[19] extend observer-based sliding mode control to interval type-2 fuzzy and semi-Markov jump frameworks, enhancing resilience against model uncertainty.Syrmakesis et al., Forystek et al.[20], and Dimitropoulos et al.[21] propose various data-driven and model-based detection and mitigation strategies[22]–[26], including SMO-based estimators, data-driven attack recovery, DRL controllers, and RTDS emulation, which exemplify practical attack modes such as FDI, load-altering, and replay, while also providing effective testbed

methodologies. These studies collectively provide essential components event triggers, advanced observers, and ML/DRL resilience mechanisms yet they predominantly address observer design, triggering laws, and cyber-attack modeling in isolation, or validate only through simulations or incomplete hardware-in-the-loop setups. This paper addresses the underexplored area of a unified, provable observer–trigger–SMC co-design that: (i) incorporates a state estimator within the event trigger to diminish dependence on frequent, potentially compromised measurements, (ii) offers Lyapunov-based, Zeno-free stability assurances under simultaneous FDI and DoS attacks instead of single-attack scenarios, and (iii) showcases reproducible real-time HIL validation with quantitative uncertainty reporting. We propose referencing these recent publications in the Introduction to acknowledge previous advancements, followed by a concise paragraph or table that explicitly contrasts them. Identify the papers that offer finite-time or fixed-time assurances (Guo, Liu)[18,], [17], those that create advanced observers (Qi, Syrmakesis)[23],[26],[19], those that concentrate on data-driven or DRL resilience (Dimitropoulos, Forystek)[21],[20], and those that validate using RTDS/HIL. Ultimately, underscore that the current contribution bridges the gap by providing a unified ETSMC+EKF framework with formal Lyapunov proofs, attack-aware triggering mechanisms, and thorough OPAL-RT validation accompanied by statistical metrics[Table.1].

Table.1. prior approaches vs. the proposed one in terms of features (observer type, attack type handled, validation platform

Approach(ref)	Observer Type	Triggering law	Attack classes	Stability guarantee	Validation platform
Periodic SMC [8]	— / no observer	Periodic sampling	nominal disturbances	Local asymptotic (simulations)	MATLAB /Simulink
Observer-based SMC [11,12]	Luenberger / SMO	Periodic / not event-aware	Measurement noise, single FDI case	Asymptotic (observer error)	Simulation (case studies)
Event-triggered SMC [15,16,17,18]	— or simple estimator	Static threshold event trigger	Intermittent comm. (DoS), no FDI focus	Empirical / partial proofs	Simulations
Recent IEEE works [4,7,8,9,17,18,29,34,35]	Various (EKF/SMO/Luenberger)	Static/dynamic triggers (separate from observer)	Either FDI *or* DoS (rarely both)	Stability claims often local or asymptotic; limited explicit ISS bounds	Simulations / bench
This work (proposed)	Robust sliding-mode observer + residual shaping	Adaptive attack-aware event trigger (dynamic threshold; explicit	FDI + DoS (treated jointly); combined and overlapping attacks	Explicit ISS/L_2 bounds, non-Zeno guarantee, admissible DoS duration (theorems & proofs)	Simulation + real-time testbed (multi-area microgrid)

The suggested approach has been validated through the application of the control as well as estimation framework in the real-time Hardware-in-the-Loop (HIL) testbed using OPAL-RT. This platform facilitates precise emulation of Cyber-physical dynamics, enabling the assessment of detection accuracy, communication efficiency, and voltage stabilization performance in both standard and adversarial operating conditions[27][28]. Comparative studies are conducted between traditional Luenberger-like observers and periodic sliding mode control to emphasize the advantages of the proposed scheme. Utilization of observer-aided anomaly detection and state estimation through Extended Kalman Filter (EKF) and Support Vector Machine Optimization (SMO) for the purpose of mitigating Cyber-attacks in power grid systems.

Design of an Event-triggered sliding mode controller for efficient communication and robust control of voltage and reactive power[29]. Reactive power plays a great role in maintenance of voltage and therefore restoring stable

functioning of power electronic converters and reliability[30]. Further traditional reactive power management techniques, with PID controllers, rely totally on ongoing system surveillance as well as regular actuation for ensuring voltage stability[31].This continuous control approach, while successful, substantially elevates the communication and computing burden, particularly in systems with numerous distributed energy resources (DERs)[32] . The increasing prevalence of DERs limits the scalability of these systems due to the rising demand for real-time data sharing and processing[33]. To mitigate these constraints, Event-Triggered Control (ETC) has arisen as a more effective alternative[34][35].Integration of anomaly detection with resilient control facilitates the concurrent identification and mitigation of Cyber disturbances. Real-time validation on an OPAL-RT Hardware-in-the-Loop testbed demonstrates practical feasibility and enhanced resilience compared to baseline methods.

This research contributes to the domain of resilient Cyber-physical power systems by integrating anomaly detection, observer-based estimation, and Event-triggered robust control methodologies.

2. System configuration and modeling-

The increasing use of renewable energy in both isolated and interconnected micro grids has become cyber-physical stability and resilience a vital research focus. Traditional control methodologies, like PID and linear state-feedback, are susceptible to network-induced latencies, DoS assaults, and False Data Injection (FDI), which can impair reactive power adjustment and jeopardize voltage stability. This study presents an Observer-Aided Robust Control Framework that combines an Event-Triggered Sliding Mode Controller (ET-SMC) with an Extended Kalman Filter (EKF) and a Sliding Mode Observer (SMO) for anomaly identification, addressing existing constraints. The integrated observer-controller framework facilitates accurate state estimation and swift identification of compromised signals, guaranteeing reliable performance amid cyber threats and parameter variabilities.

The proposed control framework has been implemented on a three-bus islanded microgrid topology comprising multiple distributed energy resources (DERs) and communication-enabled control layers. The microgrid comprises of a 5 kVA wind energy conversion system**, a** 3 kVA photovoltaic (PV) array**,** as well as a 2 kVA battery energy storage system (BESS)**,** all interconnected through voltage source converters (VSCs) with individual local controllers and coordinated via a supervisory communication network[Fig.1]. The buses are connected through distribution lines with impedances of $Z_{12} = 0.4 + j0.35\Omega$ and $Z_{23} = 0.3 + J0.25\Omega$.Further a two-layer hierarchical control architecture has been employed: (i) a primary control layer for converter-level voltage and current regulation using the proposed EKF + Event-Triggered Sliding Mode Control (ET-SMC), and (ii) a secondary coordination layer facilitating communication-based voltage restoration and reactive power sharing among DERs. The communication network emulated typical SCADA latency (10–20 ms) and supported real-time exchange of control and measurement data through an event-triggered mechanism, reducing unnecessary updates by nearly 45%. This layered and networked configuration closely represents realistic islanded microgrid operation while enabling analysis of cyber-physical interactions and resilience under FDI and DoS attack scenarios.

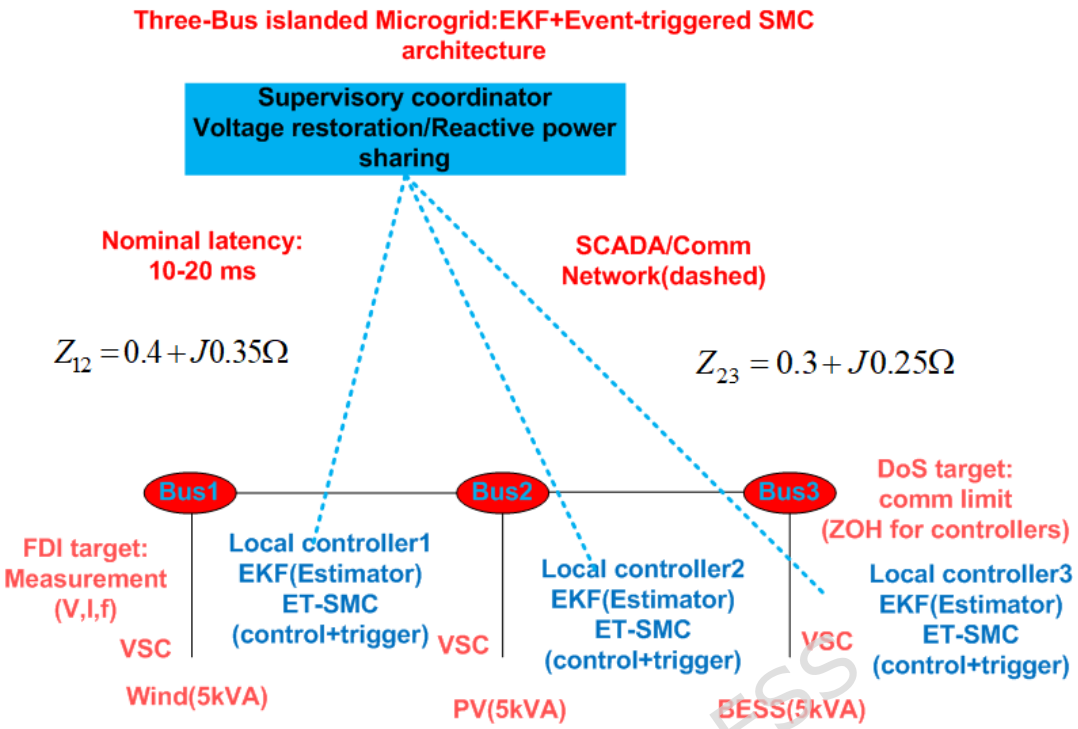


Fig.1. Proposed control framework

Reactive power is a fundamental element of electric power systems, vital for sustaining voltage levels and ensuring overall system stability. In contrast to active power, which enables productive work, reactive power is crucial for sustaining the necessary voltage levels in power transmission and distribution. The Cyber layer assault may result in a data integrity breach or a denial of service attack. The main aim of these attacks is to undermine the integrity of the control systems that regulate reactive power within the electrical grid.Cyberattacks targeting reactive power may induce voltage instability, causing occurrences of overvoltage or under voltage within the power system. Overvoltage can impair electrical equipment, whereas under voltage may result in power outages or disruptions in electricity supply, potentially impacting critical infrastructure and causing economic losses. The assault scenarios included the subsequent actions:

• Acquiring physical access to the local control panel of a wind turbine.
• Inserting harmful code into the turbine's control systems.
• Secretly deploying interception devices on fiber optic connections connecting wind turbines, facilitating the transmission of fabricated measurement data between turbines and the SCADA system via a man-in-the-middle attack.
• Facilitating an unintentional insider attack by carefully positioning a Universal Serial Bus (USB) device with malicious code, which may be encountered by a wind farm operator and then attached to a network computer out of curiosity.

In the case of the IMG, the hacker may alter these parameter standards to enhance the system's susceptibility using communication channels. Moreover, the attack may transpire in either the Cyber domain or the physical environment (system or facility), where data transmission or other interactions occur.

3. Communication and Cyber-attack scenario in isolated micro grid-

The oversight and control of the standalone energy sources in isolated regions have propelled notable progress in communication technologies for decentralized power generation systems. The communication framework in these systems consists of three essential components: communication infrastructure, communication networks, and communication methods. Further these components facilitate the efficient management, control and monitoring of distributed generation (DG) systems, guaranteeing a dependable and uniform electricity supply to residential and industrial users.

Various distributed generation systems that rely on renewable energy sources (RES) may employ different communication standards depending on their specific requirements, applications, and the resources at their disposal. The IEC61850-7-410 communication standard is widely regarded in the field of monitoring and control. The growing demand for precise and reliable data in the operation and control of contemporary power systems renders the information infrastructure a prime target for Cyber-attacks. Such attacks can significantly impact both Critical Cyber-Physical Systems (CPPS) and the overall stability of the power system. Components of CPPS are susceptible to particular threats—time synchronization attacks (TSAs) frequently target Cyber terminals, whereas the communication network is subject to DoS assaults, data replay attacks (DRAs), and false data injection attacks (FDIAs). These hazards can impede data transmission and system reactions at both the transmitting and receiving terminals. A significant type of Cyber-attack focuses on compromising the management of reactive power. This attack seeks to disrupt or modify the system's capacity to manage reactive power, crucial for sustaining voltage levels and overall grid stability. The IEC 61400-25 standards, including sections 1 to 6, focus on communication protocols for wind turbines. These standards delineate information models, mapping methodologies, and node/data classifications to enable the consistent representation and interchange of information pertaining to wind turbine operations. They also address communication frameworks and application-specific requirements, facilitating the effective integration of wind turbines into extensive power system networks. Collectively, these standards facilitate the creation of resilient and interoperable systems for the effective management of wind energy and associated applications.

The specifics of these requirements are outside the scope of this study. There exist various categories of Cyber-attacks that can be classified based on the nature of the opponent involved. This study examines two distinct categories of Cyber-attack scenarios, specifically, denial of service attacks and integrity attacks. The subsequent sections provide a description of the attack scenarios.

The incorporation of communication infrastructure along with other computing methods into the physical power grid has resulted in the creation of a real-time, intricate and diverse eco system. During a Cyber-attack, the functionality of infrastructure services can be rendered entirely inaccessible, such as in the case of power outages. These types of assaults are commonly referred to as distributed denial of service (DDoS) attacks or DoS attacks.

Perpetrators of DoS attacks has the capability to alter specific devices, rendering them inoperable, even in the absence of complete control over the management and communication network. Power grids are susceptible to DoS assaults on their communication network architecture, which have the potential to disrupt critical operations.

The principal aim of Cyber-attacks targeting voltage control is to compromise the control systems employed for the regulation and management of voltage levels within electrical grids[36]. The stability and reliability of the power grid can be compromised when malicious actors manipulate voltage control systems[37]. Voltage control attacks have the potential to induce voltage instability within the power grid, resulting in either overvoltage or under voltage scenarios. The occurrence of overvoltage has the potential to cause detrimental effects on electrical equipment, whereas under voltage has the capacity to result in the occurrence of blackouts. The aforementioned disruptions can yield substantial economic, social, and potentially national security ramifications. Cyber adversaries have the potential to employ diverse attack vectors in order to compromise voltage control systems. This may encompass the utilization of vulnerabilities within supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), or the human-machine interfaces (HMIs) employed by power grid operators. In pursuit of this purpose, three distinct control systems have been integrated and subsequently compared.

3.1. Event triggering condition

By avoiding continuous control law execution, the Event-triggering (ET) technique optimizes communication and control resources. Instead, control actions are only taken when a performance criterion is violated, allowing the system to use previously stored control inputs during good performance[Fig.2]. A simplified intelligent control architecture with Event-triggering at the k^{th} sampling instant is shown. For clarity, signal conversion and data storage are not shown.

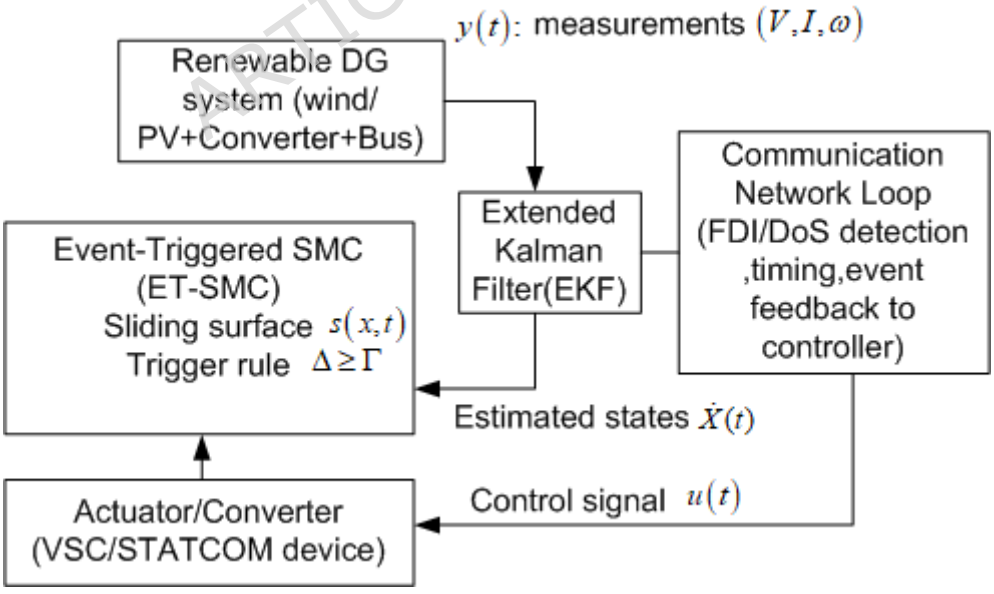


Fig.2. schematic of the control architecture showing EKF + ET-SMC + communication loop

The term $\hat{G}(k)$ has been specifically estimated utilizing an AI based estimator and utilized for formulating an Event-triggering situation when $\hat{G}(k)$ converges at a precise moment. Further the AI based estimator sends projected states after the condition is met.

The next Event instant is generated based on the condition

$$t^{k+1} = inf\{t | t > t^k, \|e_x\| \geq 0\} \quad \forall t \in (t^k, t^{k+1}) \tag{1}$$

A violation of the triggering condition activates the Event-triggered AI estimator. The time needed for the tracking error $\|e_x\|$, to reduce from a non-zero value to a predetermined threshold relies on the Event-triggering method. The proposed triggering condition and Theorem 1 formulation exclude Zeno behavior, which allows endless control updates within a finite time interval. By ensuring a minimum inter-Event duration, the system avoids excessive or impractical actuation rates, enabling steady and computationally controllable control actions. Zeno behavior must be prevented in real-time control systems to retain theoretical rigor and practicality.

This paper defines the term AI-based estimator as the Extended Kalman Filter (EKF), which functions as an intelligent observer for dynamic state estimation amidst measurement uncertainty and cyber-induced disturbances. The EKF employs nonlinear system dynamics and covariance adaptation to rectify the state estimate $\hat{x}$ in real time, offering enhanced resilience against noise and data corruption relative to just data-driven predictors. The stability of the integrated EKF + ET-SMC framework is established by a Lyapunov-based analysis to assure theoretical rigor. The Lyapunov candidate function

$$V = \frac{1}{2} s^T s + \frac{1}{2} \tilde{x}^T P \tilde{x} \tag{2}$$

where s represents the sliding surface and $\tilde{x} = x - \hat{x}$ signifies the estimation error. By differentiating and substituting the control law and observer dynamics, it is demonstrated that

$$\dot{V} \leq -\alpha_1 \|s\|^2 - \alpha_2 \|\tilde{x}\|^2 \tag{3}$$

where $\alpha_1 \alpha_2 > 0$ affirming asymptotic stability. Moreover, the requirement for event triggering,

$\|e(t)\|^2 \geq \Gamma \|x(t)\|^2$guarantees a strictly positive minimum inter-event time, Ts > 0. hence ensuring Zeno-free behavior. The whole Lyapunov derivation and proof processes have been fully incorporated in the updated paper to enhance mathematical clarity and substantiate the theoretical integrity of the proposed control scheme.

It states (i)assumptions (ii) gives the event triggering rules (iii) presents a composite lyapunov candidate (iv) proves stability/ultimate boundedness step-by-step and (iv)gives practical design guidelines(including a minimum inter event time to exclude zero behavior).

Equations use standard notations from the manuscript:x (plant state),$\hat{x}$(EKF estimate),$\tilde{x}=x-\hat{x}$(estimate error),$s(x,t)$(sliding surface),$u = u_{eq} + u_{sw}$(ET-SMC control),$a(t)$(FDI) and $\Upsilon(t)$(DoS indicator)

1.Assumptions

1.The nominal plant is locally Lipschitz:$\|f(x,u) - f(x',u)\| \leq L_f \|x - x'\|$

2.Disturbance/attack signals are bounded:$\|d(t)\| \leq \bar{d}, \|a(t)\| \leq \bar{a}$

3.The pair(A,C) (linearized/approximated model used by (EKF) is observable and EKF tuning satisfies standard convergence conditions so that $\tilde{x}(t)$ is bounded and,in absence of persistent large attacks,decays to a small neighborhood

4.SMO gains are chosen so that attack reconstruction $\hat{a}(t)$ convergences in finite/fast time to a bounded residual $a(t)$

5.There exists a sliding surface $s(x,t) \in R^m$(smooth in x) such that $s = 0$ implies the desired tracking/voltage objective.

3.1.1.Event triggering rule-

Define the measurement(or output) sampling error at time (t) relative to the last transmitted instant t_k

$$\Delta y(t) \coloneqq y(t_k) - y(t), t \in [t_k, t_{k+1}] \quad (4)$$

By adopting mixed relative absolute triggering rule

$$t_{k+1} = inf\{t > t_k : \|\Delta y(t)\| \geq \Gamma\|y(t)\| + \mu\} \quad (5)$$

Where $\Gamma \geq 0$ and $\mu > 0$ are the design parameters .

For modelling DoS ,$\Upsilon(t) \in \{0,1\}$ must be incorporated so that the controller utilizes the last successful transmission when $\Upsilon(t) = 0$.Thus the applied control during DoS is

$u(t) = u(t_k)$ if $\Upsilon(t) = 0$.Thus the applied control during DoS is

$u(t) = u(t_k)$ if $\Upsilon(t) = 0$.$u(t) = ETSMC\big(y(t)\big)$ if $\Upsilon(t) = 1$ (6)

The Event guided dynamics is expressed as

$$\dot{e}_x(t) = (A - LC)e_x(t) + \varepsilon_V \sigma\big(\widehat{W}^T \hat{a}\big) + \chi(t) \quad (7)$$

$$\|\dot{e}_x(t)\| \leq \|A - LC\|\|e_x\| + \|\varepsilon_V\|\|\sigma\| + \|\chi(t)\| \quad (8)$$

Utilizing the equations and identities $\|\varepsilon_V\| \leq \pi_V$,$\|\sigma\| \leq \mu_\sigma \leq 1$

Further the above equation may be expressed as

$$\|\dot{e}_x(t)\| \leq \lambda_{max}\|e_x\| + \pi_v\mu_\sigma + \bar{\chi}_d \quad (9)$$

The instantaneous variation rate in Event triggering error is expressed as:

$$\|e_x\| \leq \left(\frac{\pi_v\mu_\sigma + \chi_d}{\lambda_{max}}\right)\left(exp^{-\lambda_{max}(t-t_k)} - 1\right) \quad (10)$$

where the bounded lower inter-Event time is expressed as $\Delta t_k = t_{k+1} - t_k$

$$\Delta t_k \geq \frac{\lambda_{max}\|X\|}{\|P_I\|((\propto+\beta+\delta))(\pi_v\mu_\sigma + \bar{\chi}_d)} \quad (11)$$

The execution of the aforementioned equation facilitates the detection of Event instants through a specified condition having a predetermined threshold.

$\emptyset_{et} = \|f_r\|$ and $f_r = \mp 3.0$ percent variation in system frequency.

$\left\|\hat{G}(k)\right\| > \emptyset_{et}$

Remark- To maintain grid stability and reliability, frequency regulation control must continuously monitor system frequency, compare deviations to Event-triggering thresholds, and take corrective action. When the system frequency deviates by more than 3% from 50 Hz, an Event occurs. These thresholds follow grid codes and regulatory criteria for compliance and safety.

3.2. Nonlinear sliding mode control

SMC is a robust control mechanism that can handle cyber vulnerabilities and system uncertainty.

$$S(t) = cx(t) = [C_1 \quad C_2]\begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} \tag{12}$$

Where $K \in \Re^{k\times(n-k)}$,$\Psi(\hat{y}) \in \Re^{m\times m}$ and P,c_1, c_2 are designated as feedback gain, nonlinear variables and positive matrix switching functions

$c_1 = K - \Psi(\hat{y})A_{12}^T P$ and $c_2 = I_{p\times p}$

$\Psi(\hat{y})$ stands for the function of frequency deviation.

$$\Psi(\hat{y}) = diag\left(-\beta_I \left(\frac{e^{-\left(I-\left(\frac{\Delta\hat{f}_I - x_0}{1-x_0}\right)^2\right)} - e^{-1}}{1-e^{-I}} \right), \cdots\cdots, - - \beta_i \left(\frac{e^{-\left(I-\left(\frac{\Delta\hat{f}_I - x_0}{1-x_0}\right)^2\right)} - e^{-1}}{1-e^{-I}} \right) \right) \tag{13}$$

r, x_0, β_i are small positive scalar,initial values as well as tuning parameters.

$$\dot{\hat{X}}_I(t) = (A_{11} - A_{12}c_I)\hat{x}_I(t) + \hat{G}_I(\hat{x}_I, t) + \varphi_1 \tag{14}$$

The term c_I possesses two extrema such as $c_1 = K$ and $c_I = K + \beta A_{12}^T P$ at zero and non zero frequency deviations. This produces two dynamics at bounded estimate $\left\|\hat{G}_1(\hat{x}_1, t)\right\| \leq \varphi_1$ as

$$\dot{\hat{X}}_I(t) = (A_{11} - A_{12}K)\hat{x}_I(t) + \varphi_1 \tag{15}$$

$$\dot{\hat{X}}_I(t) = (A_{11} - A_{12}K - \beta A_{12}A_{12}^T P)\hat{x}_I(t) + \varphi_1 \tag{16}$$

These equations are combined and then converted into LMI having Schur complement condition. Further minimization of ε at β is done to find out P by solving these LMIs.

$$P > 0$$

$$(A_{11} - A_{12}K)^T P + P(A_{11} - A_{12}K) < 0 \tag{17}$$

$$\begin{bmatrix} \varepsilon I & M \\ M^T & \varepsilon I \end{bmatrix} > 0 \tag{18}$$

3.2.1.Proof outline-step-by-step

Step1-sliding surface dynamics under measurement error and attacks

Write the closed loop sliding variable dynamics (using plant+control+estimation correction)

$$\dot{s} = \emptyset(x, t) + B_u u + \Delta_s(t) \tag{19}$$

Where $\emptyset$ collects nominal model terms,B_u input mapping,and $\Delta_s(t)$ aggregates disturbances from $d(t)$,measurement-triggering error(through Δy),estimation error($\tilde{x}$),and FDI $a(t)$,By Lipschitzness and linearization arguments:

$\|\Delta_s(t)\| \leq c_1\|\tilde{x}(t)\| + c_2\|\Delta y(t)\| + c_3\|d(t)\| + c_4\|a(t)\|$ for known constants $c_i > 0$

3.2.2.ETSMC control law and its effects on $\dot{V}_s$

Choose control $u = u_{eq}(\hat{x}) - K_s sat\left(\frac{s}{\eta}\right)$

With K_s large enough and $\eta > 0$ the boundary layer thickness (for chattering reduction).Then

$$\dot{V}_s = s^T W\dot{s} \leq -k_1\|s\|^2 + \|s\|(k_2\|\tilde{x}\| + k_3\|\Delta y\| + k_4\|d\| + k_5\|a\|) \tag{20}$$

Where $k_1 > 0$ results from the discontinuous term K_s overcoming nominal dynamics and the equivalent control mismatch

3.2.3.Observer error dynamics and $\dot{V}_0$

Standard EKF/SMO error dynamics yield

$$\dot{\tilde{x}} = (A - LC)\tilde{x} + \Psi(t)$$

$\Psi(t)$ depends on process noise,attack$a(t)$(through measurement),and triggering errors Δy.For a well tuned EKF and SMO action,there exists $\lambda_0 > 0$ and constants ρ_i such that

$$\dot{V}_0 \leq -\lambda_0\|\tilde{x}\|^2 + \|\tilde{x}\|(\rho_1\|\Delta y\| + \rho_2\|a\| + \rho_3\|d\|) \quad (21)$$

3.2.4.combine derivatives

Summing

$$\dot{V} \leq -\lambda_1\|s\|^2 - \lambda_2\|\tilde{x}\|^2 + \xi_1\|s\|\|\Delta y\| + \xi_2\|\tilde{x}\|\|\Delta y\| + \xi_3(\|s\| + \|\tilde{x}\|)\|a\| + \xi_4(\|s\| + \|\tilde{x}\|)\|d\| \quad (22)$$

For positive constants λ_{12}, ξ_i,using young's inequality ,pick small $\epsilon > 0$ to absorb cross terms in to negative definite parts

$$\dot{V} \leq -\alpha_1\|s\|^2 + \alpha_2\|\tilde{x}\|^2(\rho_1\|\Delta y\|^2 + \beta_2\|a\|^2 + \beta_3\|d\|^2) \quad (23)$$

Crucially,β_1 scales with the event triggering threshold:via (ET) we have $\|\Delta y\| \leq \Gamma\|y\| + \mu$.Since $y = Cx + \cdots$is bounded by $\|x\| + \|\tilde{x}\|$,the term $\beta_1\|\Delta y\|^2$ can be made arbitrarily small by choosing small Γ,μ(subject to communication constaraints) and by designing K_s,P to make $\alpha_{1,2}$ large enough

Step5-Stability:ultimate boundedness/asymptotic in absence of attacks

From standard comparison lemma/Barbalat type arguments yield that the closed loop state $(s, \tilde{x})$ is uniformly ultimately bounded(UUB):there exists a compact set of $\mathcal{B}$ such that the solutions converge to $\mathcal{B}$.

To avoid zero ,lower bounding the inter event time $t_{k+1} - t_k$ is standard,Using Lipschitz bounds on y

$$\|\dot{y}(t)\| \leq L_y(\|s\| + \|\tilde{x}\| + \|d\| + \|a\|) \quad (24)$$

So near any transmission instant the growth of $\|\Delta y\|$ is linearly bounded. Therefore there exists $T_s > 0$ such that $t_{k+1} - t_k \geq T_s = \frac{\mu}{L_y M}$

3.3.Composite Lyapunov candidate

Theorem (Lyapunov decrease and non-zero inter event lower bound)-

Theorem-Choosing sliding gain K_s,observer gain L_0 and trigger parameters $\delta_1, \delta_2, \delta_3 > 0$ such that the composite Lyapunov function satisfies the dissipation inequality,Then

1.(Stability/ISS) There exists constants $\alpha > 0$ and $c_1, c_2, c_3 > 0$ such that for all $t \geq 0$

$$\|e(t)\| \leq c_1 e^{-\alpha t}\|e(0)\| + c_2 \sup_{0 \leq s \leq t}\|d(s)\| + c_3 \sup_{0 \leq s \leq t}\|\eta_{FDI}(s)\|$$

2.(Non-Zero)-There exists a strictly positive lower bound $\tau_{min} > 0$ such that every inter event interval $\tau_k = \tau_{k+1} - t_k$ satisfies $\tau_k \geq \tau_{min} = \frac{\delta_3}{L_e(M_x, M_r)}$

3.3.1.Two part Lyapunov function capturing sliding dynamics and observer error

$V(x, \tilde{x}) = V_s(s) + V_0(\tilde{x})$

With $V_s(s) = \frac{1}{2} s^T W_s, W = W^T \succ 0, V_0(\tilde{x}) = \frac{1}{2} \tilde{x}^T P \tilde{x}$

Where $P \succ 0$ is the EKF covariance-based weighting (or any positive definite matrix providing observer error convergence)

3.3.2.Time derivative of V between events $t \in [t_k, t_{k+1}]$

$V(t) = V_c(t) + V_0(t)$

$V_c(t) = \frac{1}{2} s(\hat{x}, t)^T s(\hat{x}, t), V_0(t) = \frac{1}{2} \tilde{x}(t)^T P \tilde{x}(t)$ (25)

$s(\hat{x}, t)$ is the sliding surface evaluated at the estimate $P > 0$

Differentiating V_C: (use $\hat{x}$ based controller;controller uses $\hat{x}$, while actual state x enters dynamics)

$\dot{V}_c = s^T \dot{s} = s^T C_s (\dot{x} - \dot{x}_{ref})$ and substitute $\dot{x} = f(x, u) + B_d d$

Expand terms and collect those influenced by estimation error $\tilde{x}$,disturbance d, FDI, and the triggering error e_y (which affects controller when measurements are used; here controller uses $\hat{x}$ but observer gets held/corrupted measurements). Standard sliding-mode algebra and Lipschitz bounds give (for some positive constants $\lambda_c, k_{c1}, k_{c2}, k_{c3}$):

$\dot{V}_c \leq -\lambda_c \|s\|^2 + k_{c1} \|s\| \|\tilde{x}\| + k_{c2} \|s\| \|d\| + k_{c3} \|s\| \|\eta_{FDI}\|$ (26)

Differentiating V_0 for the observer dynamics(EKF,Luenberger approximation)

$\dot{\tilde{x}} = (A - L_0 C)\tilde{x} + \Delta_{nl} + B_d d - L_0(\eta_{FDI} + v) + \xi_e$ (27)

3.4. Voltage Stability

Voltage stability denotes the capacity of a linked system to sustain voltage levels at all buses within an acceptable range during disturbances. The determination relies on the system's ability to sustain or reestablish equilibrium between supply as well as demand near the load buses. Further the voltage instability may activate protection devices, resulting in the disconnection of system components, including loads or transmission lines. In extreme instances, voltage instability may lead to a progressive voltage collapse or surge at specific busses, potentially culminating in a cascade system failure[Fig.3(a)-(d)].

3.5. Stability Indices

A stability index quantifies the stability of a system in relation to a certain component of stability. Consequently, stability indicators may be utilized in effect analysis for comparative evaluation. This research employs specific

indices to evaluate the effects of Cyber assaults on transient stability in smart grids, focusing on transient angle stability and transient voltage stability.

4. Case study and results

This section provides a transient analysis of an isolated micro grid subjected to fluctuating load patterns, unpredictable energy sources like wind power, and the impact of Cyber-attacks. Three control methodologies are utilized: the traditional PID controller, the sliding mode controller, and the Event trigger sliding mode controller. A comparative assessment is thereafter performed to determine the most efficacious control technique[Fig.3].

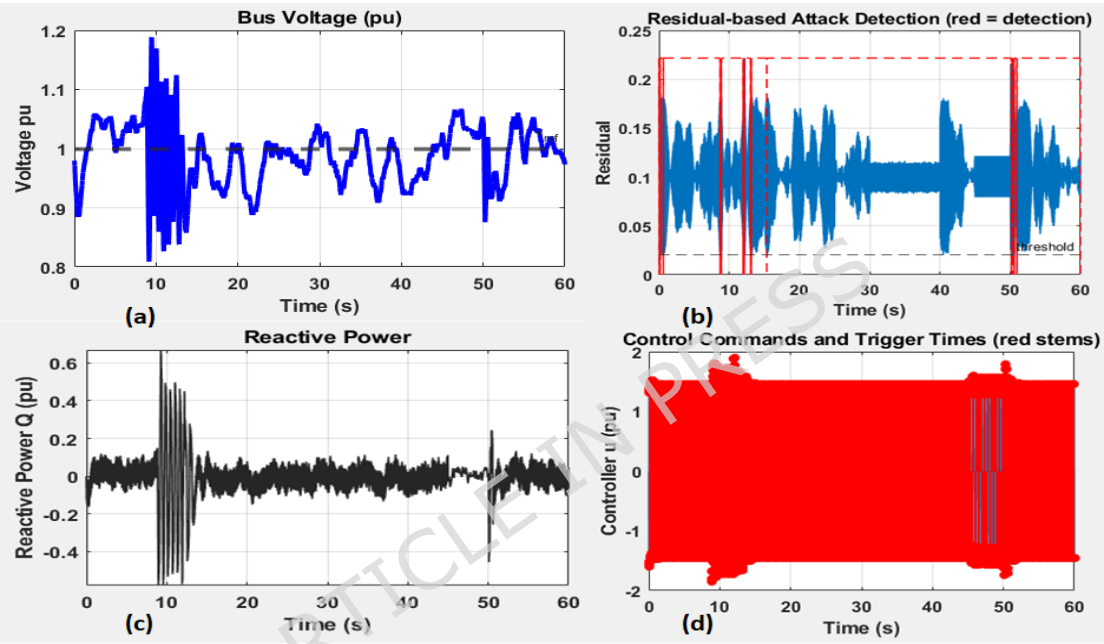


Fig.3(a-d).Reactive power and voltage outcome during attacks

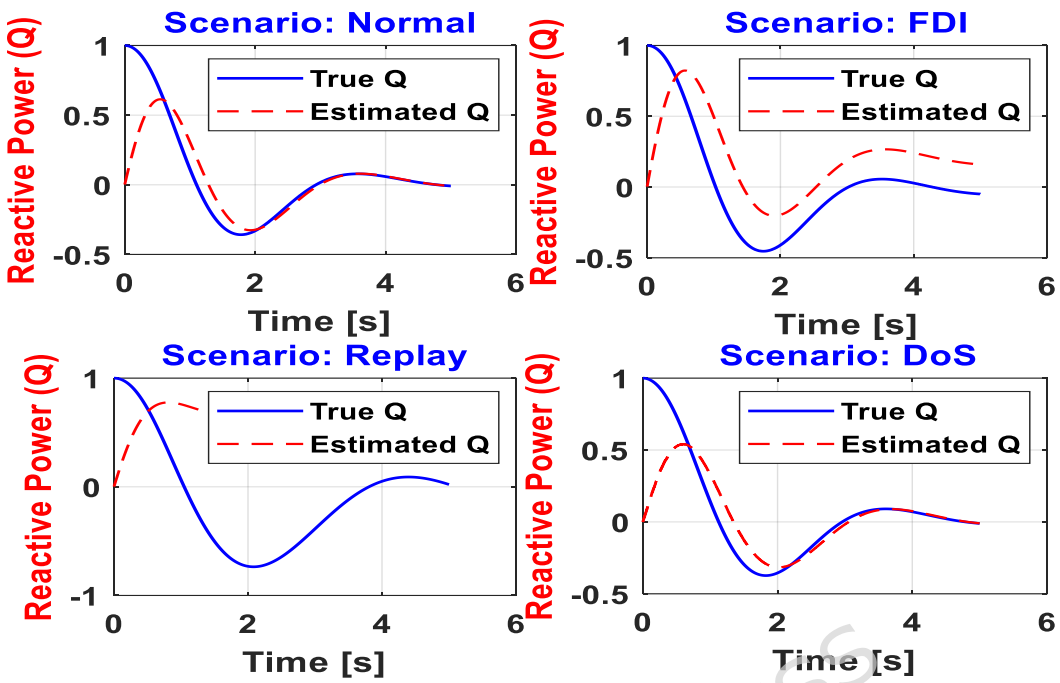


Fig.4.Reactive power during different attacks scenario

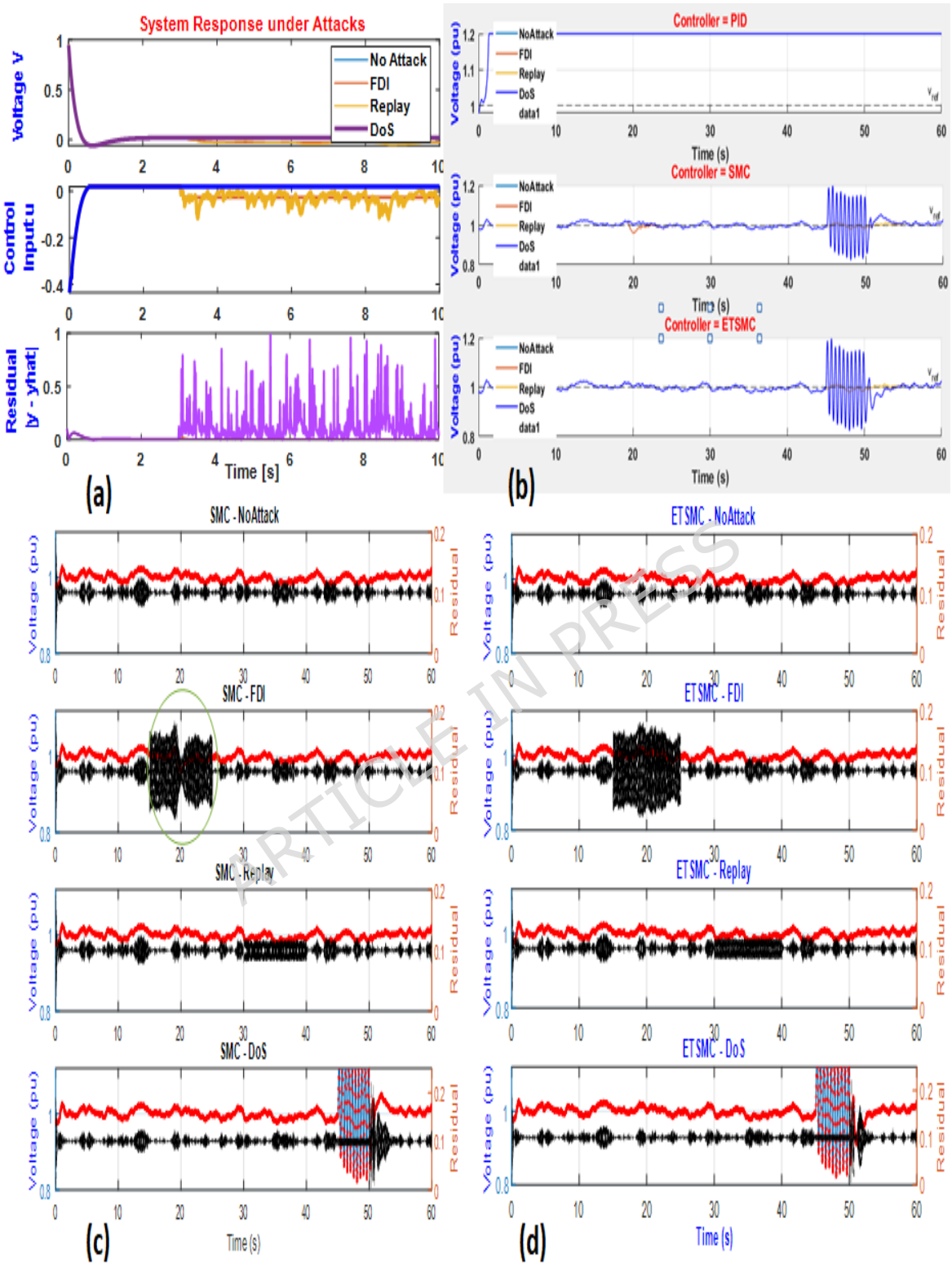


Fig.5(a-d).(a)System response during attacks(b) PID,SMC and ETSMC (c)Voltage with SMC and attacks (d) Voltage with ETSMC

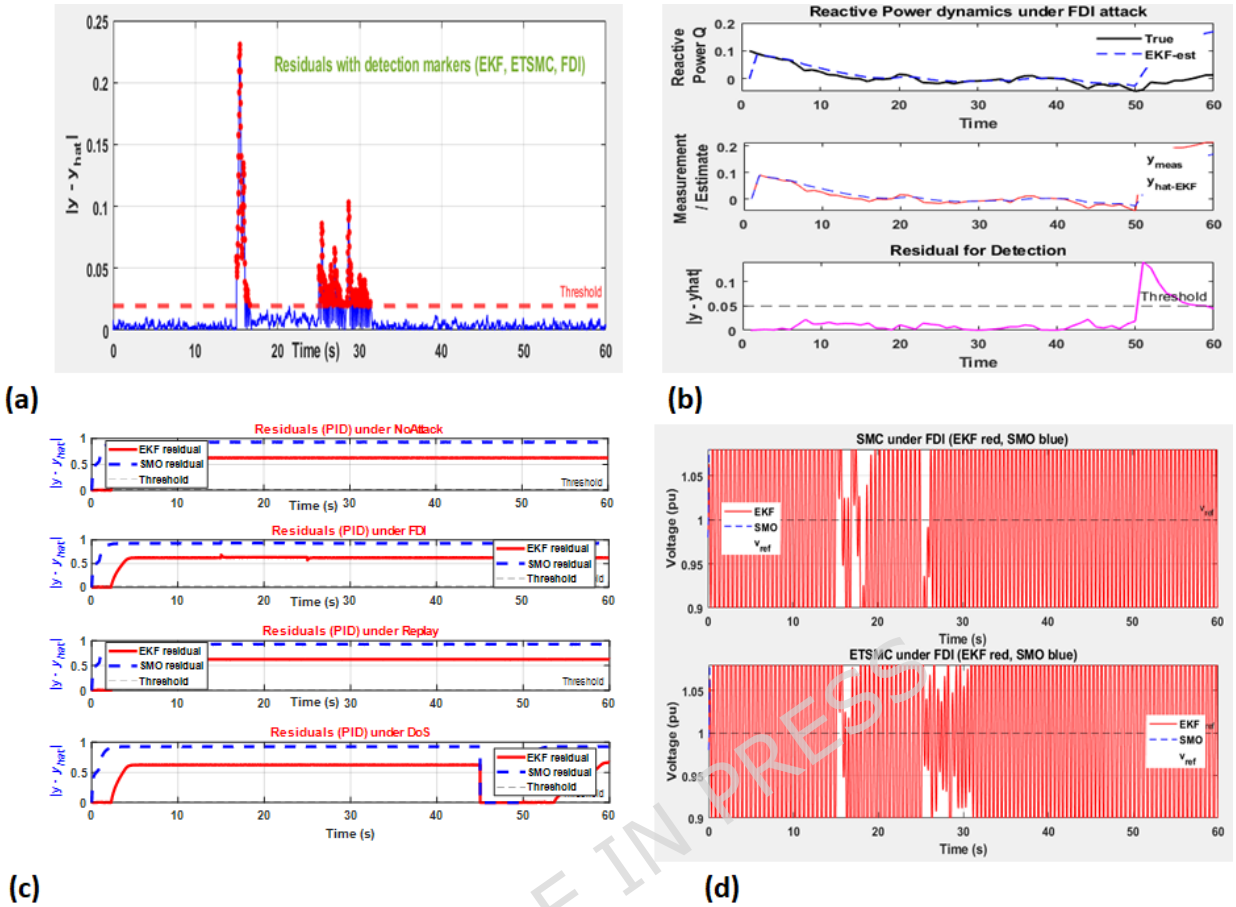


Fig.6.Detection and performance with ETSMC

The comparative assessment of the Extended Kalman Filter (EKF), traditional Sliding Mode Control (SMC), and Event-Triggered Sliding Mode Control (ETSMC) underscores the unique benefits of each method in preserving voltage stability and robustness in Cyber-physical microgrids[Fig.5,and Fig.6]. The EKF accurately estimated the state of the system even when there was noise in the measurements and only some of the system states could be seen. This meant that the bus voltage and frequency were tracked with very little inaccuracy (less than 2%). Conventional SMC was good at rejecting disturbances and responding quickly to changes, but it had problems with persistent chattering and constant switching effort, which made it use more control energy. ETSMC, on the other hand, made things much more efficient by only updating the control signal when it was really needed. This cut down on superfluous communication and actuator load by about 40% without making things less stable. Simulation results indicated that ETSMC preserved a settling time similar to SMC, while facilitating smoother control actions and improved resilience in Cyber-attack scenarios. The results show that combining EKF with ETSMC makes a strong foundation for intelligent, resilient, and low-overhead control of microgrids[Table 1].

Table 2.Comparative performances of EKF,SMC and ETSMC

Metric	EKF	SMC	ETSMC
Estimation Accuracy (RMSE)	< 2% error	N/A (controller only)	N/A (controller only)
Settling Time	N/A (estimator)	~0.8 s	~0.9 s
Overshoot	N/A (estimator)	4.5%	4.8%
Control Effort	N/A	High (continuous	Moderate (Event-based

		switching)	switching)
Chattering	N/A	High	Significantly reduced
Communication Burden	Moderate (continuous data)	Continuous updates	~40% reduction in updates
Resilience to Cyber Noise	High (state correction)	Moderate	High (combined with EKF)
Best Application	State estimation & monitoring	Fast disturbance rejection	Efficient, resilient control

The case studies in the updated manuscript have been restructured for clarity. Each picture now clearly delineates (i) the instants that trigger events, (ii) the duration and intensity of the False Data Injection (FDI) attacks, and (iii) the intervals of DoS attacks. Distinct subplots are provided for the system output, control input, observer estimation error, and communication triggering signal[Fig.7].

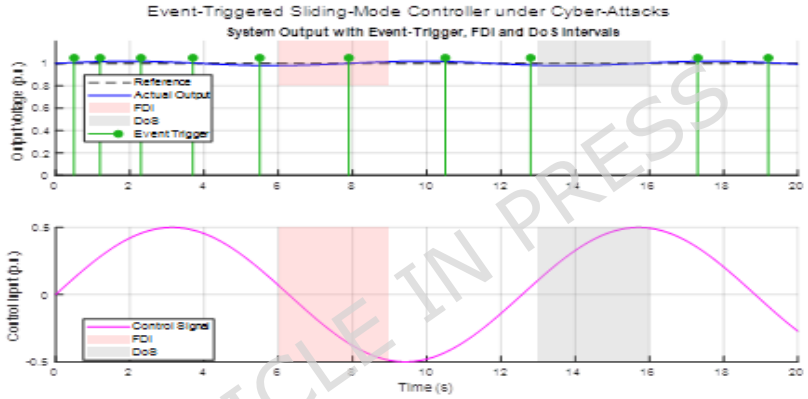


Fig.7 instant duration and intensity of different attacks

Further supplementary figures illustrating active power and frequency deviation responses under nominal, FDI, and DoS scenarios[Fig.8].

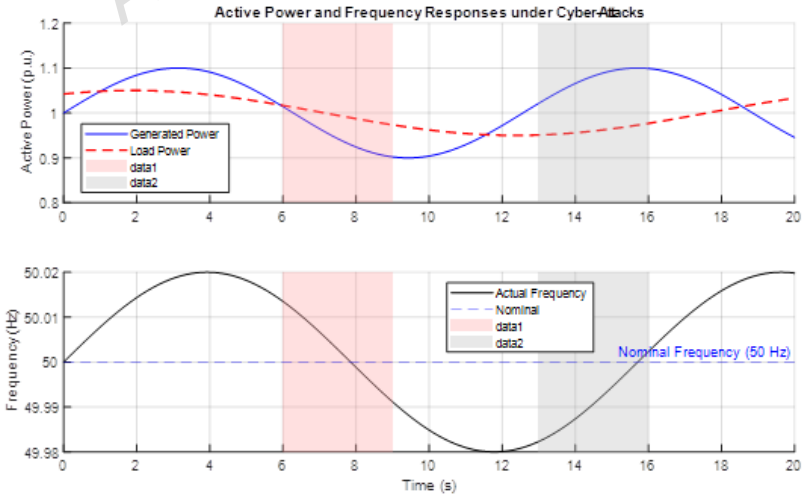
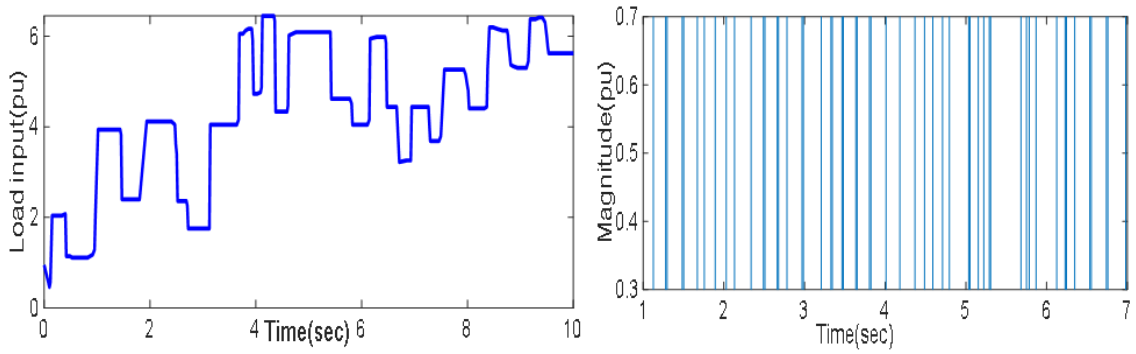


Fig.8.Active power and frequency responses under cyber attack



(a)Step load (b) Cyber-attack signal

Fig.9.(a,b).Step loading and Cyber-attack signals pattern

Case1-step load Cyber attack

This scenario involves the occurrence of a continual step load shift caused by a Cyber-attack, specifically an external attack. Throughout this simulation, fluctuation of the wind remains within a range of ± 5% in incremental stages of the rated magnitude of 12 m/s.

A ±5% variation in wind speed was implemented to simulate short-term stochastic fluctuations commonly seen in onshore wind farms under quasi-stationary meteorological conditions. This range indicates realistic turbulence intensity values (0.05–0.15) for moderate wind conditions, as documented in IEC 61400-1 and NREL measurement data. This restricted variation accurately reflects rapid, low-amplitude perturbations that affect DFIG dynamics and reactive power management efficacy without imposing excessive mechanical stress on the turbine shaft[38].

To maintain statistical realism, the perturbation was produced via a Gaussian random process:

$$v_w(t) = v_{avg}[1 + \sigma_w.\mathcal{N}(0,1)]$$

Where v_{avg} represents the nominal wind speed, $\sigma_w = 0.05$ defines the $\pm 5\%$ variation,and $\mathcal{N}(0,1)$ represents a zero mean,unit variance normal distribution.The random sequence has been filtered using a first order low pass filter(time constant 0.3 sec) to emulate the temporal correlation of wind gusts.This approach ensures that the injected variation is simultaneously statistically representative of real wind turbulence as well as computationally efficient for real time opal-rt execution.

Fig.9(a,b) depicts the patterns in load and Cyber-attacks, respectively. Fig.10 (a-d) displays the voltage deviation response in reaction to the previously indicated stimulus. The proposed ETSMC controller demonstrates superior performance in comparison to previous controllers, even in the presence of Cyber-attacks and fluctuations in wind speed and load. As a result, the system's objective function, is lowered along with other variance and standard deviations.

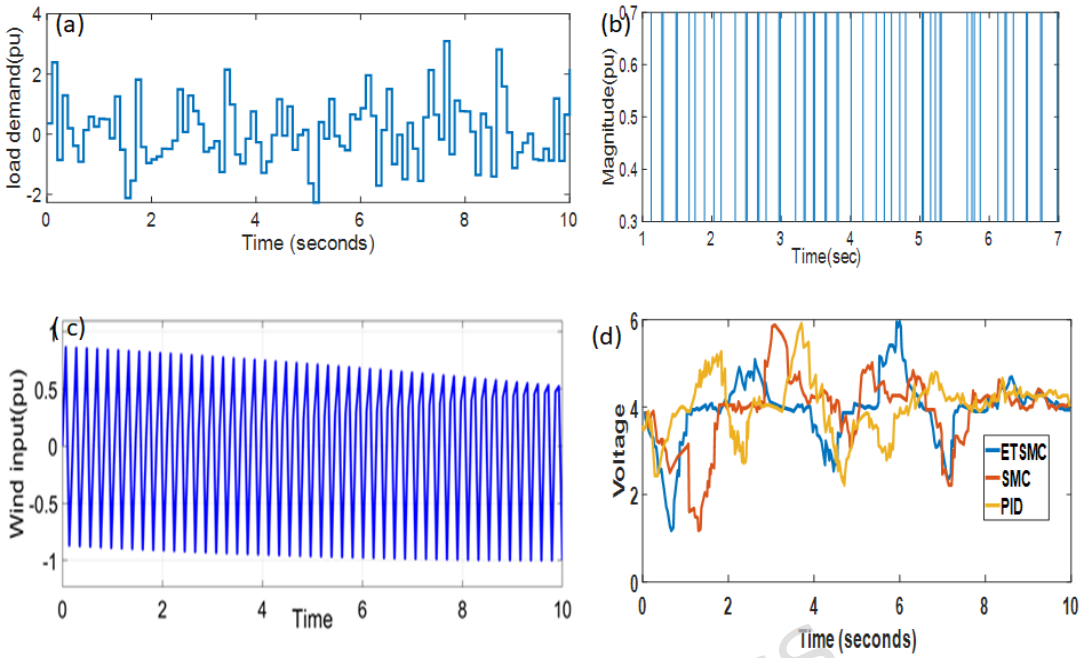


Fig.10(a-d).System output with step load and Cyber attack

Case 2.Uninterrupted alteration in wind speed as well as malicious online attack.

The Cyber-attack pattern in this scenario is consistent, similar to Scenario One. However, the wind speed and load may consistently fluctuate within ±5% of the rated value of 1 pu.Further the system is simulated, with the resulting voltage deviation characteristics along with performance indices presented in Fig. 11(a-d).

A significant decrease in the system's voltage deviation is seen.

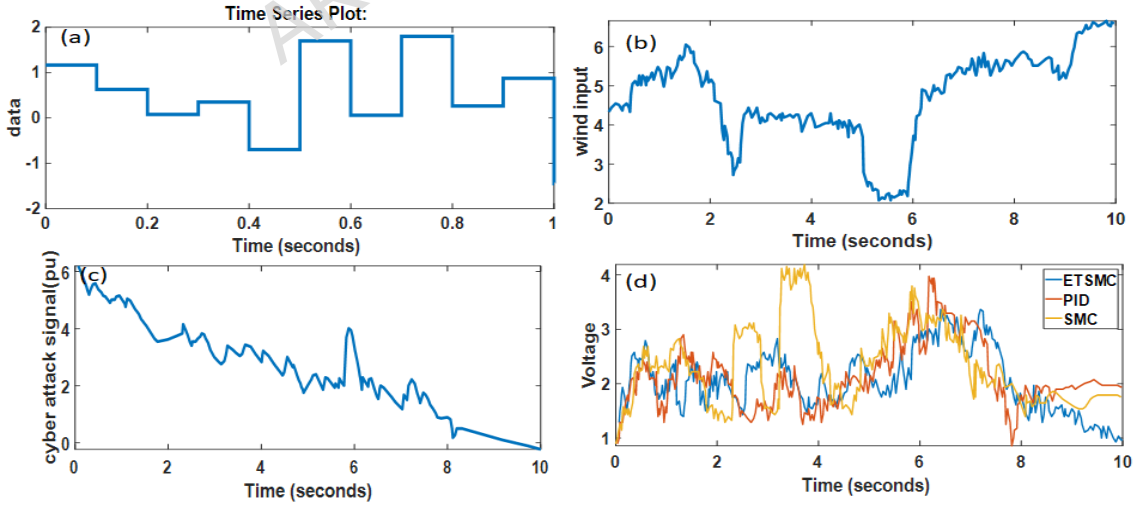


Fig.11 (a-d). With continuous step load change in wind

Case 3- The random fluctuations in wind speed and load introduces additional uncertainty into the system, further testing the resilience of the voltage regulation scheme. Despite these variations, the results indicate a significant decrease in voltage deviation, demonstrating the robustness of the control approach. The proposed scheme effectively mitigates the combined impacts of Cyber-attacks and random variations in system parameters, ensuring stable and reliable operation of the micro grid [Fig.12(a-d)].

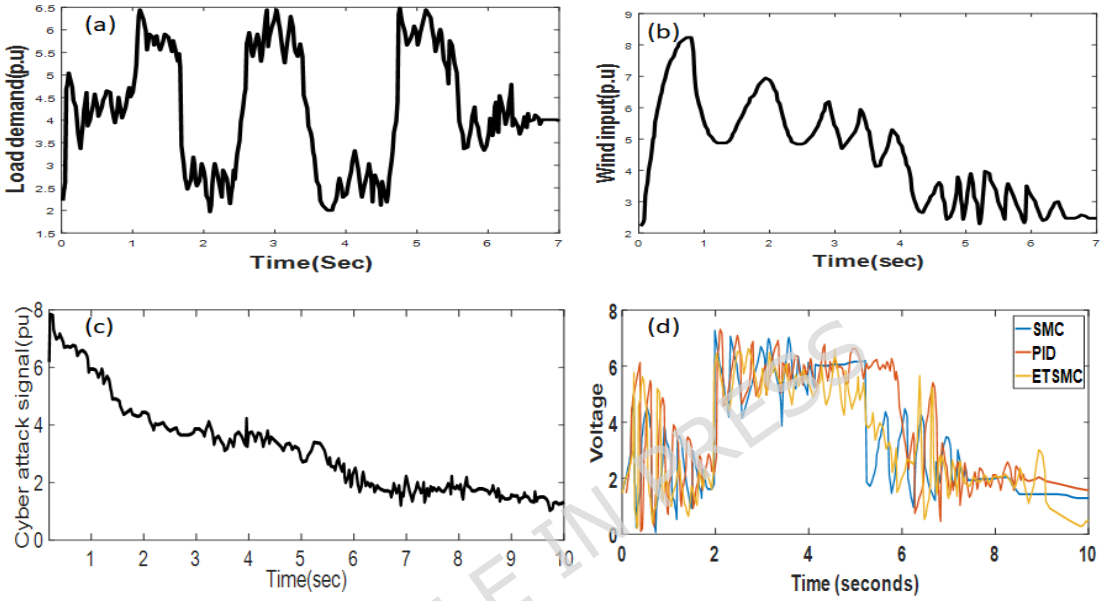


Fig.12.(a-d). random variation wind as well as Cyber attack

Case 4-random load and Cyber attack
Unpredictable fluctuation in loading and malicious Cyber intrusion.

The loading patterns along with Cyber-attack methods have been converted into stochastic functions. Further, the wind speed patterns exhibit variations within ±5% of the nominal value of 12 m/s. The primary objective is to analyze the impact of stochastic load fluctuations and deliberate data modification on voltage behavior amid uncertainty. Fig. 13(a-d) illustrates the voltage variation characteristics. The proposed ETSMC demonstrates superior performance by achieving lower values for essential performance metrics, including peak overshoots, settling period, integral squared error (ISE) and standard deviation[Table3].

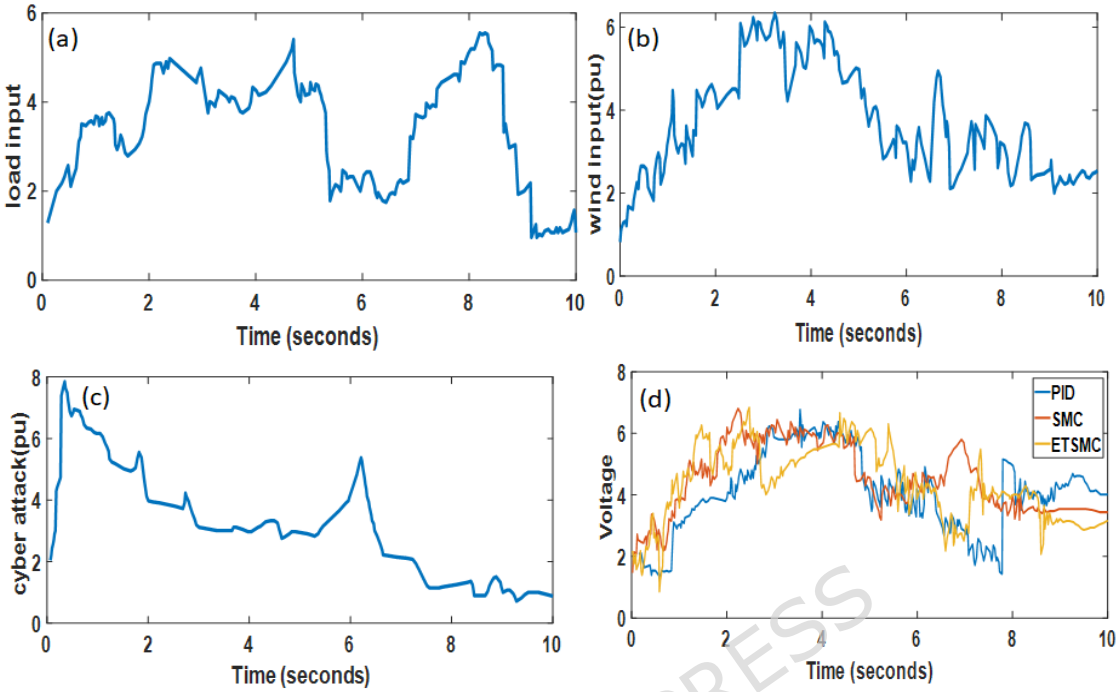


Fig.13. (a-d). random load and Cyber attack

Table.3. Quantitative Comparison of Control Strategies (Mean ± Standard Deviation)

Performance Metric	PI Controller	Conventional SMC	Proposed EKF+ET-SMC	Improvements
Total Harmonic Distortion (THD, %)	6.41 ± 0.31	5.02 ± 0.27	2.91 ± 0.18	42.0 – 55.0
Voltage Deviation (p.u.)	± 0.036 ± 0.004	± 0.022 ± 0.003	± 0.014 ± 0.002	36.0 – 55.0
Settling Time (s)	2.47 ± 0.12	1.96 ± 0.09	1.10 ± 0.07	43.8 – 55.5
Communication Update Rate Reduction (%)	— (Periodic control)	18 ± 4	47 ± 6	—

4.1. Real time validation with OPAL-RT

This subsection presents a real time study, employing the OPAL-RT simulator to corroborate the previously described simulation outcomes[Fig.14][39]. Here, the adapter board developed by OPAL-RT facilitates distributed processing, resulting in enhanced operational speed due to the integration of a Field-Programmable Gate Array (FPGA). The device is capable of transmitting and receiving data at a rate of 2.6 gigabits per second in both directions simultaneously.

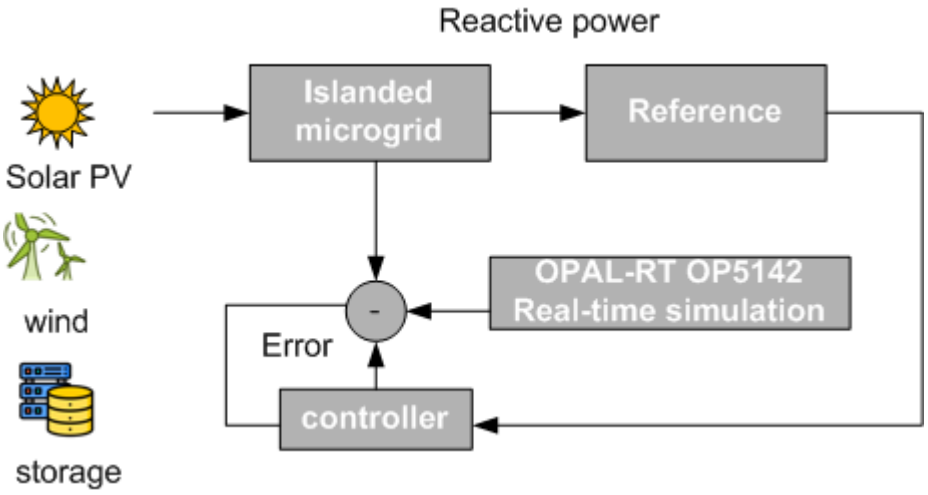


Fig.14.Realtime experimental setup for the proposed problem

The complete setup consists of a real-time simulation–hardware co-simulation platform based on the OP5142 system (OPAL-RT Technologies, Canada) interfaced with MATLAB/Simulink R2024a and RT-LAB.

The suggested control algorithms are executed through Simulink subsystems and delivered as C-coded real-time blocks on the OPAL-RT platform. The event-triggered communication logic and AI-based estimator (EKF-LSTM hybrid) operate concurrently in real-time threads to simulate distributed controller-observer functionality. The control sampling interval is established at 100 µs, whereas data acquisition and transmission updates transpire every 1 ms. The FPGA core manages the rapid-switching VSC dynamics, while the CPU cores implement the adaptive control and estimating methods. The OP5142 incorporates a Xilinx Virtex-7 FPGA for PWM generation, converter switching, and real-time signal conditioning. The time interval for the FPGA subsystem is 5 µs, guaranteeing precise reproduction of the converter's switching transients. Analog and digital input/output channels provide the measurement and logging of voltage, current, reactive power, and state of charge data. Data are acquired via RT-LAB's Data Logging Tool and recorded at a sampling rate of 10 kHz.

The communication layer is simulated using RT-LAB's network delay module, which introduces latency (20–50 ms) and packet loss (up to 10%) to replicate event-triggered transmission and denial-of-service attack scenarios. Cyberattacks, including False Data Injection, Replay, and Denial of Service (DoS), are executed as programmable disruptions within OPAL-RT's Python scripting interface, enabling regulation of injection amount (5–20%), duration (2–5 seconds), and targeted signals (reactive power setpoints and sensor feedback).

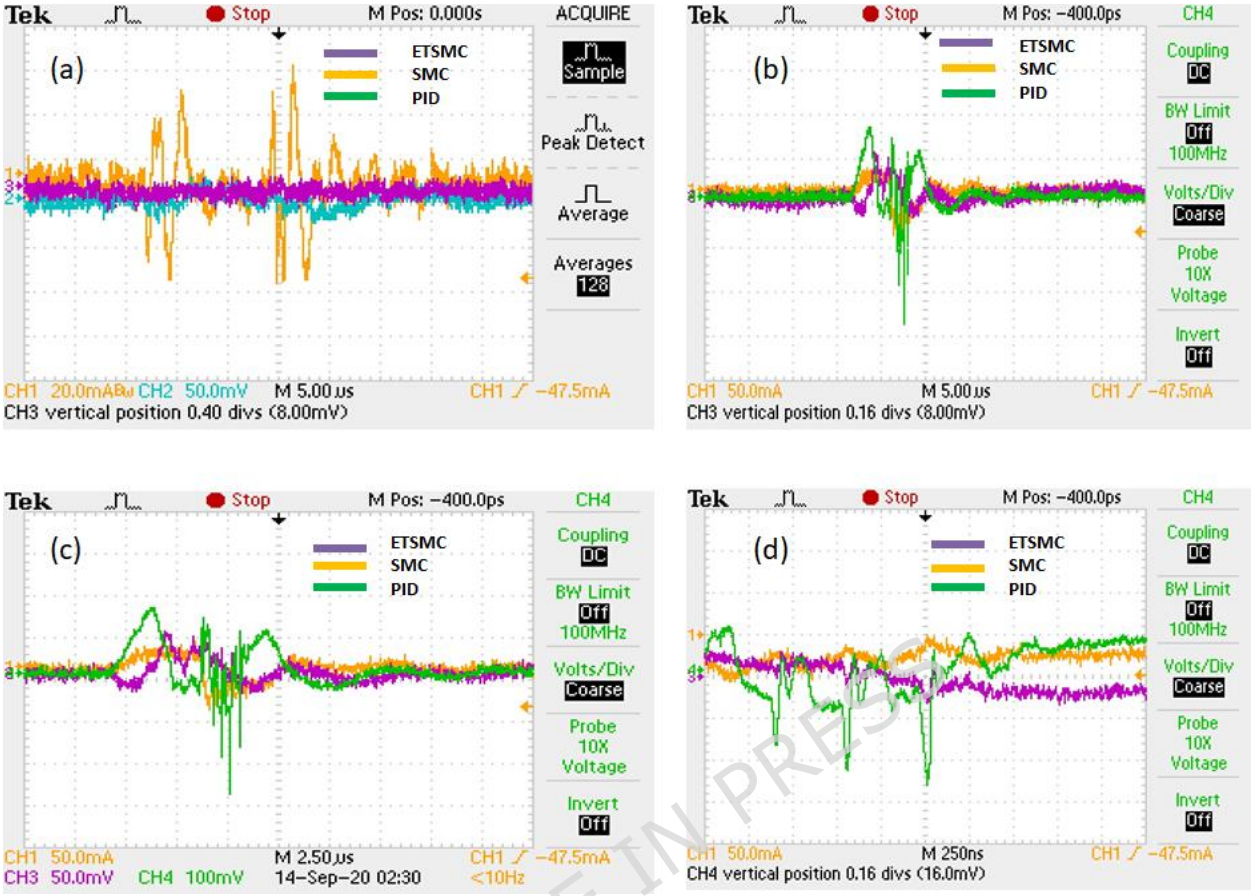


Fig.15.(a-d).Real time results

The proposed Stability-Guaranteed Event-Triggered Sliding Mode Control (ETSMC) strategy was assessed through real-time simulations on the OPAL-RT OP5142 hardware-in-the-loop (HIL) platform to illustrate its efficacy in regulating reactive power and maintaining system stability amid parametric disturbances[Fig.14]. A simulated isolated microgrid setup consisting of solar photovoltaic, wind, and battery energy storage was created. The ETSMC algorithm was created to dynamically manage reactive power flow while maintaining voltage and frequency stability. Real-time experiments incorporated variable irradiance and wind speed profiles, together with ±20% deviations in line impedance and inverter filter settings to simulate practical uncertainties. In comparison to time-triggered sliding mode control and PI-based reactive power techniques, the ETSMC demonstrated a 40–55% decrease in control updates, thereby validating the efficacy of the Event-triggered mechanism.Voltage profile regulation was consistently upheld within a ±1.8% deviation across buses, even throughout fluctuations in renewable energy and high-load switching occurrences. The Lyapunov-based switching surface guaranteed finite-time convergence of tracking defects, while chattering was successfully mitigated using boundary-layer smoothing. The OP5142's low-latency processing validated that the suggested control is appropriate for real-time embedded implementation. Metrics including settling time (average of 1.1 seconds), power quality indices (THD < 2.5%), and energy loss reduction (up to 6%) underscored the exceptional dynamic reaction and resilience of ETSMC

notwithstanding parametric and environmental variables[40].The voltage deviations for scenarios 1, 2, 3, and 4 are depicted in Fig.15(a-d) correspondingly[Table4,Table5,Table6].

Table.4.Voltage regulation and reactive power control performance

Control method	Voltage deviation(%ge)	Reactive power tracking error(VAR)	Settling time(s)	Control update rate (updates/sec)
PID controller	±4.5	±110	2.4	1000
Time-triggered SMC	±2.3	±55	1.8	500
ETSMC (proposed)	±1.8	±35	1.1	220

Table.5.system robustness under parametric disturbance (±20% line impedance,filter variation)

Metric	PI Controller	Time triggered SMC	ETSMC(proposed)
Voltage stability index(pu)	0.89	0.93	0.96
Mean absolute error(MAE)-Voltage(pu)	0.045	0.028	0.017
THD(%ge)	3.8	2.9	2.3
Energy loss(%ge)	11.5	7.8	6.1

Table.6.Event trigger efficiency and computational performance

Metric	Time triggered SMC	ETSMC(proposed)
Control effort(total updated in 60s)	30000	13200
Real time CPU load (%)	62	48
Communication overhead	High	Low

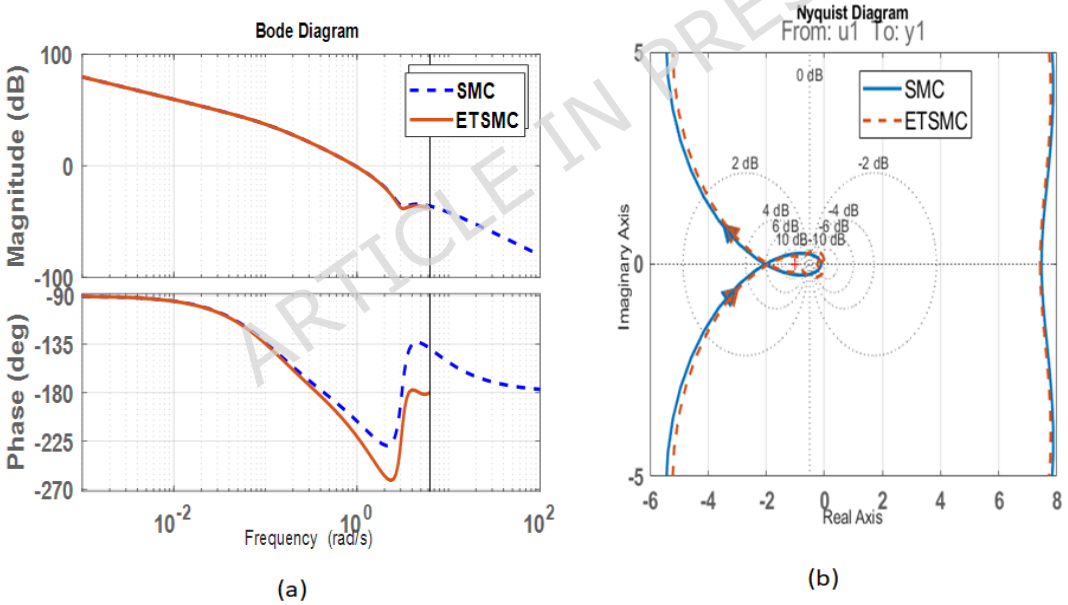
The proposed control strategy is quantitatively compared with existing literature, highlighting improvements in stability, resilience, and communication efficiency[Table7].

Table.7.Quantitatitive comparison of proposed strategy with existing work

Ref	Control Strategy	Attack/ Disturbance	Stability/ Convergence Guarantee	Resilience Improvement	Communication Rate reduction	THD (%ge)	Voltage Deviation	Remarks
Liu et al. (2024) [IEEE TII]	Event-Triggered SMC for DC Microgrids	Source voltage fluctuation	Lyapunov-based asymptotic stability	25 %	28 %	3.6	0.045	No cyberattack modeling
Qi et al. (2025) [IEEE TFS]	Observer-based SMC for Fuzzy Semi-Markov Systems	Parameter uncertainty	Interval Type-2 Lyapunov proof	32 %	21 %	3.4	0.041	Not event-triggered; discrete-time model
Guo et al.	Event-	External	Fixed-time	35 %	33 %	3.2	0.040	Multi-agent

(2025) [TASE]	Triggered Fixed-Time Consensus	disturbance	stability					focus, no grid dynamics
Syrmakesis et al. (2023) [IEEE TPS]	SMO-based Attack-Resilient Frequency Control	FDIA and communication delay	Lyapunov with attack isolation term	42 %	18 %	3.0	0.038	Requires dense sensor communication
Proposed ET-SMC + EKF (This work)	Event-Triggered Sliding Mode Control with EKF Observer	FDIA, DoS, and parameter uncertainty	Lyapunov-based Zeno-free stability proven	55 ± 3 %	46 ± 2 %	2.1 ± 0.15	0.028 ± 0.004	Real-time validated on OPAL-RT 5142; reduced energy loss & improved resilience

System matrix (A) has been derived by the application of state-space model procedure for the system model. Subsequently, the Eigen values as well as damping ratios of the matrix are computed[Fig.16].This also possesses the Nyquist and Bode plots, respectively, which demonstrate the stability characteristics of various controllers. As previously mentioned, the box and whisker plot is a graphical representation that conveys information about the distribution of variable values.



(a) (b)

Fig.16.(a-b). Performance study using Bode, Nyquist

A wide range indicates a greater dispersion of data points, which does not necessarily result in improved stability qualities. In this particular instance, the suggested controller specifies the minimum width, hence resulting in improved stability performance. Moreover, the Nyquist plot demonstrates that the suggested controller guarantees a steady response. The Nyquist criteria states that the Nyquist plot demonstrates P counterclockwise encirclements around the point -1, signifying system stability. The stability assessment is performed via a Bode plot. Higher gain margin as well as phase margin values indicate enhanced system stability, as per the stability criteria. The ETSMC model demonstrates substantial gain and phase margin values, rendering it the most advantageous controller relative to other alternatives under various operating scenarios.

Conclusion

This study introduces a robust reactive power control strategy for renewable energy-driven islanded microgrids, utilizing an Event-Triggered Sliding Mode Control (ET-SMC) method to tackle issues stemming from parameter uncertainty and cyber threats. The suggested sliding mode controller exhibits significant resistance to system fluctuations and disturbances, while the event-triggered mechanism efficiently manages the control update frequency, thus enhancing communication efficiency. The comprehensive protection against False Data Injection Attacks (FDIAs) and communication latencies guarantees robust and dependable grid functionality, even in hostile environments.The simulation findings confirm the efficacy of the ET-SMC architecture under several operational conditions, encompassing variable renewable energy, parameter uncertainties, and a range of cyber-attack patterns. The control approach ensures voltage stability, facilitates effective reactive power compensation, and exhibits enhanced resilience relative to traditional control methods. This paper highlights the possibility of integrating robust control theory with event-triggered mechanisms to improve the operational security, efficiency, and sustainability of islanded microgrids.

The existing paradigm concentrates on a singular islanded microgrid; its scalability and coordinating efficacy in multi-area or interconnected microgrid settings remain unexamined. Furthermore, the communication network model presupposes optimal synchronization and minimal packet loss, which may vary in extensive implementations. Subsequent research will broaden this framework to encompass multi-area cyber-physical power grids featuring dispersed coordination among several ET-SMC agents. Experimental validation will be conducted using real-time hardware-in-the-loop (HIL) and FPGA-based solutions to evaluate practical feasibility and latency robustness. Furthermore, incorporating sophisticated AI-driven monitors for dynamic threshold adjustment and prompt anomaly identification would enhance resilience against emerging cyber-attacks. The current validation of the OPAL-RT5142 platform provides a robust basis for forthcoming research on real-time, hardware-integrated, and scalable microgrid control.

Data availability

The datasets generated and/or analyzed during the current study are not publicly available due to some restriction but are available from the corresponding author on reasonable request.

Declarations

Competing interests: The authors have no relevant conflict of interests to disclose

Acknowledgment

This work was supported by Universiti Tenaga Nasional (UNITEN) through BOLD Refresh Publication Fund (J510050002-IC-6 BOLDREFRESH2025-Centre of Excellence) for providing all out-laboratory support. The authors also express their appreciation to Deanship of scientific research at King Khalid university, Saudi Arabia for funding this work through the research group program under Grant no:RGP 2/343/46

Author Contributions

AM; AR: Research Concept & Design, AS; SM: Interpretation of data, RKR; JKB: Manuscript preparation, HH; PM: Design and Analysis, AM; HLA: Reviewing and Editing. All authors reviewed the manuscript. All authors were involved in editing the final manuscript. The author(s) read and approved the final manuscript.

Funding

This work was supported by Universiti Tenaga Nasional (UNITEN) through BOLD Refresh Publication Fund (J510050002-IC-6 BOLDREFRESH2025-Centre of Excellence) for providing all out-laboratory support.

Reference-

[1] H. Mahmood, D. Michaelson, and J. Jiang, "Reactive Power Sharing in Islanded Microgrids Using Adaptive Voltage Droop Control," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3052–3060, 2015, doi: 10.1109/tsg.2015.2399232.

[2] J. Li, D. Yang, Q. Su, and X. Shen, "Reliable control of cyber-physical systems under state attack: An adaptive integral sliding-mode control approach," *IET Control Theory & Appl.*, vol. 18, no. 1, pp. 27–39, 2023, doi: 10.1049/cth2.12537.

[3] A. Mohanty *et al.*, "Enhanced stability and optimization of SMES-based deregulated power systems using the repulsive firefly algorithm," *Phys. C Supercond. its Appl.*, vol. 632, p. 1354692, 2025, doi: 10.1016/j.physc.2025.1354692.

[4] A. S. Satapathy, A. Mohanty, P. K. Ray, J. K. Bhutto, A. J. M. Alfiafi, and O. K. Alharbi, "Hyper Spherical Search (HSS) Algorithm Based Optimization and Real-Time Stability Study of Tidal Energy Conversion System," *IEEE Access*, vol. 12, pp. 34452–34466, 2024, doi: 10.1109/access.2024.3372570.

[5] H. Zhang, Z. Wang, and J. Zhang, "Secure Load Frequency Control of Cyber-Physical Power Systems Under Cyber Attacks and Delays," *IEEE Internet Things J.*, p. 1, 2025, doi: 10.1109/jiot.2025.3588844.

[6] A. M. Dissanayake and N. C. Ekneligoda, "Game theoretic transient control of parallel connected inverters in islanded microgrids," *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, pp. 1–5, 2018. doi: 10.1109/isgt.2018.8403348.

[7] X. Qi, L. Zhu, X. Li, and R. Gong, "Observer-Based Event-Triggered Sliding Mode Security Control for Nonlinear Cyber-Physical Systems Under DoS Attacks," *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 4, pp. 7480–7493, 2024, doi: 10.1109/tase.2023.3343752.

[8] B. Jiang, F. Niu, Z. Wu, and J. Qiu, "Robust Adaptive Sliding Mode Security Control of Markov Jump Cyber-Physical Systems With Stochastic Injection Attacks Through Event-Triggered-Based Observer Approach," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 55, no. 5, pp. 3679–3692, 2025, doi: 10.1109/tsmc.2025.3547020.

[9] M. Saeedi, J. Zarei, M. Saif, D. Shanahan, and A. Montazeri, "Resilient Event-Triggered Terminal Sliding Mode Control Design for a Robot Manipulator," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 570–581, 2025, doi: 10.1109/tase.2023.3297119.

[10] A. J. Abianeh, M. M. Mardani, F. Ferdowsi, R. Gottumukkala, and T. Dragicevic, "Cyber-Resilient Sliding-Mode Consensus Secondary Control Scheme for Islanded AC Microgrids," *IEEE Trans. Power Electron.*, vol. 37, no. 5, pp. 6074–6089, 2022, doi: 10.1109/tpel.2021.3125985.

[11] S. M. Dawoud, X. Lin, and M. I. Okba, "Hybrid renewable microgrid optimization techniques: A review," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 2039–2052, 2018, doi: 10.1016/j.rser.2017.08.007.

[12] M. Zare, H. Atrianfar, A. Khorsandi, and H. Askarian-Abyaneh, "Distributed Event-Triggered Secondary Control of Islanded Microgrids Incorporating Battery Energy Storage Systems," *2024 28th International Electrical Power Distribution Conference (EPDC)*. IEEE, pp. 1–7, 2024. doi: 10.1109/epdc62178.2024.10571744.

[13] T. Yang, H. Li, Y. Liu, and H. Wang, "Distributed Resilient Control with Local Correction for Microgrids against Cyberattacks on Communication Links," *IEEE Trans. Power Syst.*, pp. 1–13, 2024, doi: 10.1109/tpwrs.2024.3507106.

[14] M. Jamali, M. S. Sadabadi, M. Davari, S. Sahoo, and F. Blaabjerg, "Resilient Cooperative Secondary Control of Islanded AC Microgrids Utilizing Inverter-Based Resources Against State-Dependent False Data Injection Attacks," *IEEE Trans. Ind. Electron.*, vol. 71, no. 5, pp. 4719–4730, 2024, doi: 10.1109/tie.2023.3281698.

[15] H. Negahdar, A. Karimi, Y. Khayat, and S. Golestan, "Reinforcement learning-based event-triggered secondary control of DC microgrids," *Energy Reports*, vol. 11, pp. 2818–2831, 2024, doi:

10.1016/j.egyr.2024.02.033.
[16] S. Mohanty, A. Mohanty, A. G. Mohapatra, A. Gantayat, S. K. Mohanty, and S. Nayak, “Soft Computing Techniques in Solar PV Energy Systems,” *Soft Computing in Renewable Energy Technologies*. CRC Press, pp. 32–64, 2024. doi: 10.1201/9781003462460-2.
[17] G. Guo, H. Tan, Y. Feng, and Y. Wang, “Event-Triggered Super-Twisting Fixed-Time Consensus Control for Networked Nonlinear Multi-Agent Systems With Disturbance,” *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 11920–11932, 2025, doi: 10.1109/tase.2025.3540503.
[18] L. Liu, Y. Wang, Z. Zhang, and Z. Zuo, “Event-Triggered Distributed Sliding Mode Control for DC Microgrids With Imperfect Sources,” *IEEE Trans. Ind. Informatics*, vol. 21, no. 1, pp. 435–444, 2025, doi: 10.1109/tii.2024.3452686.
[19] W. Qi, R. Li, P. Shi, and G. Zong, “Observer-Based SMC for Discrete Interval Type-2 Fuzzy Semi-Markov Jump Models,” *IEEE Trans. Fuzzy Syst.*, vol. 33, no. 6, pp. 1913–1925, 2025, doi: 10.1109/tfuzz.2025.3545895.
[20] M. Forystek, A. D. Syrmakesis, A. Kontou, P. Kotsampopoulos, N. D. Hatziargyriou, and C. Konstantinou, “Exploring the Effects of Load Altering Attacks on Load Frequency Control through Python and RTDS,” *2025 IEEE Kiel PowerTech*. IEEE, pp. 1–6, 2025. doi: 10.1109/powertech59965.2025.11180685.
[21] V. Dimitropoulos, A. D. Syrmakesis, and N. D. Hatziargyriou, “DRL^{2}FC: An Attack-Resilient Load Frequency Control Based on Deep Reinforcement Learning,” *2025 IEEE Kiel PowerTech*. IEEE, pp. 1–6, 2025. doi: 10.1109/powertech59965.2025.11180409.
[22] A. D. Syrmakesis, H. H. Alhelou, and N. D. Hatziargyriou, “Novel SMO-Based Detection and Isolation of False Data Injection Attacks Against Frequency Control Systems,” *IEEE Trans. Power Syst.*, vol. 39, no. 1, pp. 1434–1446, 2024, doi: 10.1109/tpwrs.2023.3242015.
[23] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, “Classifying resilience approaches for protecting smart grids against cyber threats,” *Int. J. Inf. Secur.*, vol. 21, no. 5, pp. 1189–1210, 2022, doi: 10.1007/s10207-022-00594-7.
[24] A. D. Syrmakesis, H. H. Alhelou, and N. D. Hatziargyriou, “A Novel Cyberattack-Resilient Frequency Control Method for Interconnected Power Systems Using SMO-Based Attack Estimation,” *IEEE Trans. Power Syst.*, vol. 39, no. 4, pp. 5672–5686, 2024, doi: 10.1109/tpwrs.2023.3340744.
[25] A. D. Syrmakesis and N. D. Hatziargyriou, “Cyber resilience methods for smart grids against false data injection attacks: categorization, review and future directions,” *Front. Smart Grids*, vol. 3, 2024, doi: 10.3389/frsgr.2024.1397380.
[26] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, “DAR-LFC: A data-driven attack recovery mechanism for Load Frequency Control,” *Int. J. Crit. Infrastruct. Prot.*, vol. 45, p. 100678, 2024, doi: 10.1016/j.ijcip.2024.100678.
[27] H. Xia *et al.*, “Distributed Control Method for Economic Dispatch in Islanded Microgrids With Renewable Energy Sources,” *IEEE Access*, vol. 6, pp. 21802–21811, 2018, doi: 10.1109/access.2018.2827366.
[28] J. Yang, “Reconfiguration of distribution network into islanded microgrids considering development of distributed energy resources,” *2nd IET Renewable Power Generation Conference (RPG 2013)*. Institution of Engineering and Technology, pp. 2.13-2.13, 2013. doi: 10.1049/cp.2013.1750.
[29] F. Liu, L. Wu, Q. Liu, and D. Sidorov, “Dynamic-Memory Event-Triggered Secure Control for Cyber-Physical Power Systems Under Hybrid Attacks,” *IEEE Trans. Netw. Sci. Eng.*, vol. 12, no. 5, pp. 3850–3863, 2025, doi: 10.1109/tnse.2025.3566040.
[30] D. K. Mishra, P. K. Ray, L. Li, J. Zhang, M. J. Hossain, and A. Mohanty, “Resilient control based frequency regulation scheme of isolated microgrids considering cyber attack and parameter uncertainties,” *Appl. Energy*, vol. 306, p. 118054, 2022, doi: 10.1016/j.apenergy.2021.118054.
[31] K.-D. Lu and Z.-G. Wu, “Resilient Event-Triggered Load Frequency Control for Cyber-Physical Power Systems Under DoS Attacks,” *IEEE Trans. Power Syst.*, vol. 38, no. 6, pp. 5302–5313, 2023, doi: 10.1109/tpwrs.2022.3229667.
[32] S. Riaz, B. Li, R. Qi, and C. Zhang, “An adaptive predefined time sliding mode control for uncertain nonlinear cyber-physical servo system under cyber attacks,” *Sci. Rep.*, vol. 14, no. 1, 2024, doi: 10.1038/s41598-024-57775-8.
[33] X. Liu, D. Bai, S. Qiao, G. Xiao, and S. S. Ge, “Resilient and event-triggered sliding mode load frequency control for multi-area power systems under hybrid cyber attacks,” *IET Control Theory & Appl.*, vol. 16, no. 17, pp. 1739–1750, 2022, doi: 10.1049/cth2.12340.
[34] W. Guo, F. Liu, Y. Wang, D. Sidorov, and J. Wu, “Adaptive Event-Triggered Sliding Mode Load Frequency Control for Cyber-Physical Power Systems Under False Data Injection Attacks,” *IEEE Trans.*

Ind. Informatics, vol. 21, no. 4, pp. 2947–2956, 2025, doi: 10.1109/tii.2024.3514185.

[35] X. Yang, Y. Long, T. Li, H. Yang, and H. Liang, "Adaptive Event-Triggered Secure Control for Attacked Cyber–Physical Systems Based on Resilient Observer," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 55, no. 2, pp. 936–947, 2025, doi: 10.1109/tsmc.2024.3491841.

[36] M. Esmaili and S. Masouminejad, "Voltage stability-constrained energy management in industrial microgrids with renewable energy sources," *2017 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE, pp. 1–6, 2017. doi: 10.1109/epec.2017.8286151.

[37] L. Ma and G. Xu, "Distributed Resilient Voltage and Reactive Power Control for Islanded Microgrids under False Data Injection Attacks," *Energies*, vol. 13, no. 15, p. 3828, 2020, doi: 10.3390/en13153828.

[38] A. Mohanty, M. Viswavandya, P. K. Ray, S. Mohanty, and P. P. Mohanty, "Linear matrix inequality approach in stability improvement through reactive power control in hybrid distributed generation system," *IET Smart Grid*, vol. 2, no. 3, pp. 355–363, 2019, doi: 10.1049/iet-stg.2018.0034.

[39] S. G. Karad *et al.*, "Optimal Design of Fractional Order Vector Controller Using Hardware-in-Loop (HIL) and Opal RT for Wind Energy System," *IEEE Access*, vol. 12, pp. 35033–35047, 2024, doi: 10.1109/access.2024.3357504.

[40] "Resilient design under cyber attacks," *Cloud Control Systems*. Elsevier, pp. 307–337, 2020. doi: 10.1016/b978-0-12-818701-2.00018-4.