IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Journal Européen des Systèmes Automatisés
Vol. 57, No. 3, June, 2024, pp. 639-651
Journal homepage: http://iieta.org/journals/jesa

A Machine Learning-Based Smart Grid Protection and Control Framework Using Kalman Filters for Enhanced Power Management

Prakyath Dayananda[1], Mallikarjunaswamy Srikantaswamy[2*], Sharmila Nagaraju[3], Mahendra Hanumanapura Nanjundaswamy[2]

[1] Department of Electrical and Electronics Engineering, SJB Institute of Technology, Bangalore 560060, India
[2] Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bangalore 560060, India
[3] Department of Electrical and Electronics Engineering, Sri Jayachamarajendra College of Engineering, Mysore 570006, India

Corresponding Author Email: pruthvi.malli@gmail.com

https://doi.org/10.18280/jesa.570301

Received: 19 December 2023
Revised: 10 May 2024
Accepted: 24 May 2024
Available online: 25 June 2024

Keywords:
machine learning, smart grid, power management system, kalman filter, renewable energy

ABSTRACT

Recent years have seen an increase in electrical crises due to the proliferation of automated inductors and electrical applications such as electric vehicles and mobile devices. The greater dispersion in the smart grid exposes it to risks like cyber-attacks, attenuation, and faulty detections that were not prevalent in conventional methods. The proposed machine learning-based renewable energy smart grid protector and controller (ReSGPC) using Kalman filters effectively controls and detects noise faults, cyberattacks, and attenuation, addressing the mentioned problems. Additionally, the proposed method has increased the efficiency of the smart grid due to its superior performance compared to conventional methods. This method provides an additional layer of protection for the system, safeguarding grid information. An optimal control law is developed to ensure the stability of the power network. The controller demonstrates significant improvements in effectiveness regardless of the initial values. Numerical simulations verify the developed approach, showing that the recommended method offers a more powerful line of attack. This strategy provides a crucial energy management framework for the smart grid, representing a reliable and system-based communication infrastructure with applications integrating renewable resources. Performance analysis reveals substantial improvements, with the proposed method achieving an efficiency increase of 0.25%, 0.42%, 0.32%, and 0.34% in Mean Squared Error (MSE) for Δ_1, Δ_2, Δ_3, and Δ_4 scenarios respectively, compared to existing methods.

1. INTRODUCTION

The advancement of microgrid protection and control is significantly bolstered by the development of reliable smart grid communication systems. Microgrids, essentially small-scale versions of the larger electrical grid, can operate independently or in conjunction with the traditional grid. Their growing importance is highlighted in the context of increasing renewable energy integration, demand for energy reliability, and the pursuit of greater energy efficiency. Smart grid communication systems play a pivotal role in this scenario, offering robust real-time monitoring and management capabilities. They enable seamless integration of renewable energy sources, efficient energy distribution, and quick response to fluctuations in energy demand and supply. These systems also incorporate advanced cybersecurity measures to protect against potential cyber threats, ensuring the safe and secure operation of microgrids. The evolution of microgrid protection and control through smart grid communications is not just a technical upgrade; it represents a significant shift towards more sustainable, resilient, and efficient energy systems capable of meeting the dynamic needs of modern electricity consumers [1-5].

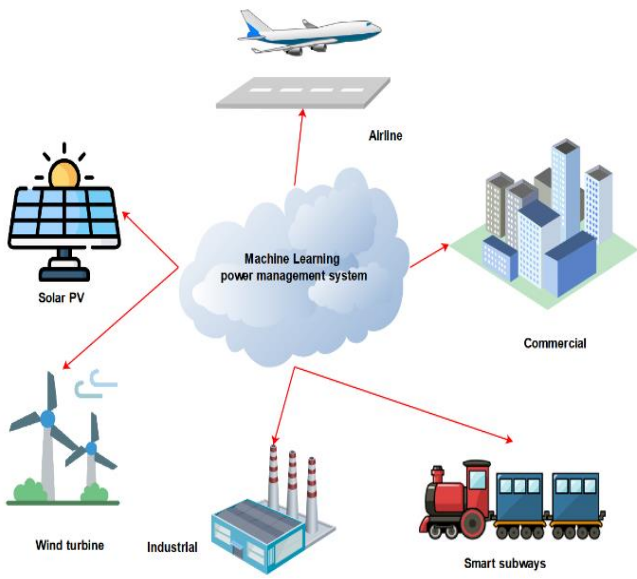

Figure 1. The fundamental structure of machine learning based power management system

Despite significant advancements in microgrid protection and control through reliable smart grid communication systems, several research gaps remain. First, there is a need for more comprehensive strategies to address the cybersecurity vulnerabilities inherent in increasingly interconnected and digitalized grid systems. As microgrids become more integrated with renewable energy sources and IoT devices, they become more exposed to cyber-attacks, necessitating advanced security protocols. Another gap lies in the development of universal standards and protocols for communication technologies in microgrids. The lack of standardization leads to compatibility and interoperability issues, hindering the efficient exchange of data and control commands among different systems and devices. Furthermore, there is a need for improved real-time data analytics and control algorithms capable of managing the complexities of distributed energy resources and fluctuating demand-supply scenarios in microgrids. Additionally, the integration and optimal management of energy storage systems within microgrids require further research, particularly in the context of variable renewable energy sources. Finally, more work is needed in designing economically viable models and regulatory frameworks that can support the widespread adoption and sustainable operation of smart grid-enabled microgrids. Figure 1 shows the fundamental structure of machine learning based power management system [6].

Renewable energy smart grid communication systems represent a cutting-edge fusion of technology and sustainable energy practices. These systems are designed to efficiently manage and distribute renewable energy resources, such as solar and wind power, through an intelligent network. By utilizing advanced communication technologies, smart grids are able to monitor energy production, distribution, and consumption in real-time, ensuring optimal efficiency and reliability. This integration not only supports the transition towards cleaner energy but also enhances the overall stability and performance of the electrical grid [7].

Our proposed machine learning-based renewable energy smart grid protector and controller (ReSGPC) using Kalman filters aims to address these gaps. The ReSGPC effectively controls and detects noise faults, cyberattacks, and attenuation, addressing the mentioned problems. Apart from this, the proposed method increases the efficiency of the smart grid due to its superior performance compared to conventional methods. The proposed method provides the system with an additional layer of protection that safeguards grid information. A develop an optimal control law to ensure the stability of the power network and perform conversion specifically on the performance index for control within the context of a convex semidefinite programming exercise [8-10]. Regardless of the initial values, the controller can function effectively, demonstrating significant improvements in the controller's effectiveness. Numerical simulations verify the developed approach, showing that the recommended method offers a more powerful line of attack. This strategy provides a crucial energy management framework for the smart grid, representing a reliable and system-based communication infrastructure with applications integrating renewable resources.

Problem statement

Recent advancements in smart grid technology have underscored the critical need for robust protection and control systems, especially with the increasing integration of renewable energy sources. However, the proliferation of automated inductors, electric vehicles, and mobile devices has exposed smart grids to new risks such as cyber-attacks, signal attenuation, and faulty detections that were not prevalent in conventional systems. Existing methods struggle to effectively address these challenges, leading to inefficiencies and vulnerabilities within the smart grid infrastructure. There is a significant demand for an advanced system that can enhance the efficiency, stability, and security of smart grids while seamlessly integrating renewable energy sources.

Research gaps

Despite significant progress in smart grid communication systems and microgrid protection, several research gaps remain. Firstly, as smart grids become more interconnected and digitalized, they are increasingly susceptible to cyber-attacks. Existing security protocols are inadequate to protect against sophisticated cyber threats, necessitating advanced and comprehensive cybersecurity strategies. Secondly, the lack of universal standards and protocols for communication technologies in microgrids leads to compatibility and interoperability issues, hindering the efficient exchange of data and control commands among different systems and devices. Thirdly, there is a need for improved real-time data analytics and control algorithms capable of managing the complexities of distributed energy resources and fluctuating demand-supply scenarios in microgrids. Additionally, further research is required for the optimal integration and management of energy storage systems within microgrids, particularly in the context of variable renewable energy sources. Lastly, more work is needed to design economically viable models and regulatory frameworks that support the widespread adoption and sustainable operation of smart grid-enabled microgrids.

Addressing these gaps, the proposed machine learning-based renewable energy smart grid protector and controller (ReSGPC) using Kalman filters aims to enhance the efficiency, stability, and security of smart grids, providing a robust solution for modern energy management. These points are elaborated in the manuscript and supported by references and figures, emphasizing the critical need for advanced smart grid protection and control mechanisms.

2. RELATED WORK

As global electricity demand rises, continents will transform their smart grids infrastructure into super smart grids (SSGs), interconnecting their power system networks to meet future demands. The SSGs system uses current technology, digital communication, machine learning, and information approaches to make the power generating system more precise and balance demand and supply. SSGs use renewable energy to support many countries' electricity systems by lowering greenhouse gas emissions. If countries cannot regulate their own demand profiles, integrating smart grids into SSGs balances demand and supply. Environment, energy management, intermittent renewable energy, and line losses are important obstacles to regular supply. This paper studied the technical obstacles of constructing futuristic SSGs for European and SAARC continents and offered a solution and discussed future research paths. Although many technical experts have praised SSG ideas, their future growth is still a research challenge due to the paucity of simulation-based

models in the literature. Finally, this research work presents a fuzzy logic hybrid cluster model of SSGs with two clusters and a renewable wind energy system to solve this problem. This approach can be used to redesign smart grids from one-country power networks to futuristic SSGs from multiple countries power networks for SAARC and Europe. MATLAB simulates clusters and wind systems. The proposed SSG concept with 18 bus networks supplies energy to two countries in two clusters whenever one or both countries in SAARC and Europe experience a problem [11].

The energy transition-revolution paradigm will provide new interaction models to efficiently manage energy and data transmitted between power system players with sustainability, resilience, cybersecurity, and privacy in mind. Demand-side management (DSM), a mix of software and hardware models with data analytics capabilities, is a key enabler of energy transactions along with switching from fossil to renewable power sources. The DSM manages the grid infrastructure to minimize customer discomfort and maximize grid stability with respect to environmental commitments, beyond demand-response. DSM techniques in modern power networks are reviewed in this article [12]. Existing DSM techniques are explained and categorized, with informative discussions to assist evaluate all studies. Future study could improve DSM in light of global data analysis/cybersecurity trends for liberalizing electricity markets based on energy transactions and DSM-based communities, especially for smart cities. Standardization, legislation, data privacy, cybersecurity, and energy system contributions were assessed as open issues in a modern DSM [13-15].

This work uses advanced machine learning to improve smart grid integration of renewable energy by projecting solar power generation for the following year. LSTM, Bi-LSTM, and AE-LSTM are used as machine learning models. These models are trained and evaluated using MAE and MSE from real-time solar power production data over a year. The hybrid AE-LSTM model captures subtle temporal patterns and correlations in the data, making it more accurate than the LSTM and Bi-LSTM models. This study shows that machine learning, particularly the hybrid AE-LSTM approach, can seamlessly integrate renewable energy resources into smart grids, making power systems more efficient and environmentally friendly. A thorough examination shows that the hybrid AE-LSTM model's additional training improves its predictions, giving it an edge over models that only use the other model's architecture [16]. This study shows that advanced machine learning methods can revolutionize renewable energy integration, with the hybrid AE-LSTM model promising improved prediction accuracy.

Modern energy systems are switching to renewables. Power electronics interfaced renewables are replacing some synchronous thermal units. Lack of natural inertia and governor damping, which are found in synchronous machines, creates concerns about system frequency stability, including rapid change and lower nadir frequency. The rapid development of communication and Internet of Things technology allows scattered energy resources to be aggregated as a virtual power plant to balance real-time electrical demand and supply. However, using the entire virtual power plant to support adjustable inertia has not been investigated [17]. The synchronous virtual power plant framework based on grid-forming inverter interfaced distributed energy resources is presented in this study. The virtual power plant supports inertia by coordinating grid-forming inverter parameters. Also develop an online learning-based parameter adjustments approach to modify virtual power plant inertia. An IEEE 34 nodes case study shows the method's efficacy [18].

Wide-area protection system (WAPS) measures electrical quantities to find smart grid problems using current sensors, communication networks, and computational technologies. The WAPS communication network sends data quickly and reliably between regional master stations and slave stations. Communication link (CL) placement substantially impacts real-time data transfer. To optimize WAPS performance, CL location should be considered along with sensible partitioning. This study extends WAPS partitioning to the simultaneous optimization problem of partitioning and optical CL placement. Formalizing the simultaneous optimization problem reduces WAPS construction costs. To enable reliable and real-time data transmission, the optimization problem captures the link bandwidth and cost of each optical CL in addition to its location and division. Final numerical simulations are performed on IEEE 39-bus, 57-bus, and 118-bus standard testing situations. The optical CL technique can be non-negligible and severely affect WAPS partitioning, according to simulations [19].

Advanced monitoring and communication technologies are digitizing the historical power infrastructure into a smart grid. IEC 61850 power grid automation standards are common. Modernizing the electrical grid increases cyberattack risk. False data injection attacks against generators in IEC 61850 compliant systems are a new cyber hazard that has not been well researched. Attack vectors against automated control logic for parallel generators and their practicality are studied, and simulation studies show the attack impact. Using the identified attack vectors, offer an efficient message authentication mechanism. For attack vector enumeration, A examine real-world control logic from the cutting-edge smart grid test-bed. Also develop an IEC 61850-compliant virtual test-bed for simulation study. Implementing and intensively evaluating the proposed message authentication techniques shows their advantages over others. Although it counters the identified attack vectors, the suggested message authentication system reduces delay by 16% compared to IEC 62351 standards [20].

Information security is receiving attention in research communities such smart grid, control, signal processing, and communication [21]. Numerous state estimate algorithms have been presented for estimating system states during cyber-attacks. The weighted least squares (WLS) method is commonly used for detecting poor data and estimating state [22, 23]. When measurement error variances are known, this technique accurately estimates system state [24].

Cyberattacks like bogus data injection can bypass faulty data detection, causing security and downtime issues. [25, 26] demonstrate the least trimmed squares strategy, which targets the Jacobian matrix and measurements. Current research explores Bayesian and Neyman-Pearson-based cyber-attack detection and state estimation [27]. A Bayesian formulation is used to provide an optimal detection and estimation technique after establishing the cost function. Using the Neyman-Pearson theorem, the cost function is minimized under specific hypothesis conditions [28]. Additionally, a joint likelihood ratio test and maximum likelihood estimator are commonly employed in literature. Although several state estimation frameworks have been suggested under attack scenarios, they have neglected reliable communication and its dynamic state estimation process [29].

Utility engineers cannot conduct trial-and-error at controller points to detect cyber-attacks. Therefore, a combination cyber-attack defense and state estimation technique is needed to stabilize the power network. In a scenario, attackers can manipulate system state information to convince the control center that overloaded branches have secured voltage, or change breaker statuses to indicate operating lines as open. Motivated by the need for secure EMS, this research aims to estimate dynamic system states when an adversary arbitrarily corrupts a set of sensors. The main contributions are:

- Modelled renewable microgrid for state space equation, using sensors for measurements. A recursive systematic convolutional (RSC) code defensive strategy is presented to safeguard system information from attackers by adding redundancy. This communication infrastructure is ideal for utilities due to its affordability, control, cyber security, and near-real-time two-way communication capabilities.
- Using the estimated system states and proposed reliable communication network, build an optimal feedback control law for system regulation. The control performance index is achieved by solving a convex semidefinite programming problem.
- The new strategy is validated using numerical simulations, demonstrating accurate system state estimation following impairment protection. The controller stabilizes the electricity network in just 0.03 seconds, according to results. Combining these methodologies creates a new paradigm for green energy and control engineering, enabling future communication and smart energy management system design.

3. FUNDAMENTAL MODELLING OF MICRO GRID AND CYBER-ATTACK

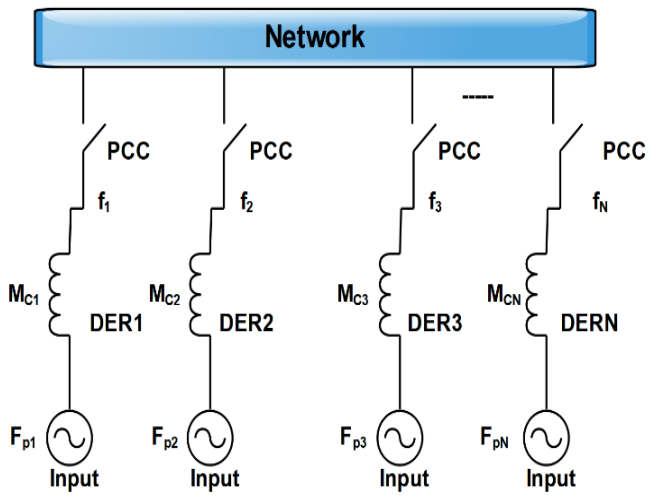

Figure 2. Fundamental structure of solar panels intergrade to the power network

In the context of the smart grid, the microgrid is a subset that extends from the substation to smart buildings and finally to individual customers. Through the use of inverters, the microgrid is connected to the power network that is comprised of limitless buses. The main grid is often connected to N distributed energy resources (DERs). Let assume, for the sake of simplicity, that N=4 solar panels are connected to one another over the IEEE-4 bus system, as depicted in Figure 2 [21, 30]. Here, the input voltages are denoted by the equation $f_p = (f_{p1}, f_{p2}, f_{p3}, f_{p4} \ldots . f_{pn})^T$, where vpi represents the i-th DER input voltage. The four solar panels are connected to the point common couplings (PCCs), and the voltages of these PCCs are represented by the equation $f_s = (f_{p1}, f_{p2}, f_{p3}, f_{p4})^T$, where, f_i is the voltage of the i[th] primary common coupling.

As of right now, the equation for the nodal voltage can be stated as in Eq. (1):

$$E(a)f_s(a) = \frac{1}{a}M_c^{-1}v_p(s) \tag{1}$$

where, the admittance matrix of the entire power network, which includes four micro-sources, is denoted by $E(a)$ and the coupling inductor $M_c = diag(M_{c1}, M_{c2}, M_{c3}, M_{c4})$. The admittance matrix is presented in Eqs. (3) and (4), and it is derived from the typical specifications of the IEEE 4-bus distribution feeder [31]. In order to obtain the discrete-time linear state space system, the following formula can be used given in Eq. (2):

$$y(k+1) = Q_d y(k) + R_d j(k) + n_d(k) \tag{2}$$

where, $y(k) = f_s - f_{ref}$ is the PCC state voltage deviation, is the PCC reference voltage, $j(k) = f_p - f_{pref}$ is the DER control input deviation, f_{pref} is the reference control effort, $n_d(k)$ is the zero mean process noise and covariance matrix is O_n, the state matrix $Q_d = I + Q\Delta\tau$ and input matrix $R_d = R\Delta\tau$ with

$$Q = \begin{bmatrix} 176.2 & 177.9 & 521 & 105.8 \\ -365 & 0 & 0 & 0 \\ -545.23 & -475.9 & -409.9 & -831.9 \\ -120.9 & -559.9 & -969.9 & -1087.6 \end{bmatrix} \tag{3}$$

$$R = \begin{bmatrix} 0.9 & 335.6 & 532.2 & -105.8 \\ -360 & 0 & 0 & 0 \\ -70.5 & -67.2 & -421.2 & -829.9 \\ -435.5 & -415.6 & -109.8 & -1088.6 \end{bmatrix} \tag{4}$$

where, $\Delta\tau$ is the discretization parameter.

A collection of sensors has been placed all around the microgrids by the utility company so that they can be monitored closely. It is therefore possible to construct a linear relationship between the measurement and the state variable is represented by Eq. (5) :

$$\mathrm{x(k)} = \mathrm{C_y(k)} + \omega\mathrm{(k)} \tag{5}$$

The measurements are denoted by $x(k)$, the measurement matrix is denoted by C, and the measurement noise with zero mean and the covariance matrix B_w are denoted by $w(\tau)$. When it comes to smart grids, the communication infrastructure usually serves the purpose of transmitting data from sensors to energy management systems (EMS). On the other hand, modern smart grids are susceptible to cyber-attacks due to the weaknesses existing inside the system. In most cases, the objective of the attacker is to introduce erroneous information into the measurements is performed by Eq. (6).

$$z(k) = C_y(k) + \omega(k) + q(k) \tag{6}$$

where, the measurements that are taken into consideration are referred to as $z(k)$, and $q(k)$ represents the fake data that was entered by the attacker [32-34]. It is predicated on the assumption that attackers have full access to the information contained within the system, which enables them to take control of, record, and change data in accordance with their own personal preferences [35]. It is interesting to note that our objective is to protect the information about the grid from being accessed by intruders so that the power system can function effectively.

4. PROPOSED SMART GRID PROTECTOR AND POWER MANAGEMENT SYSTEM

When it comes to improving efficiency, security, and reliability, the smart grid is typically expected to combine communication infrastructure, control, and processing [36]. It is possible for the communication infrastructure that supports the monitoring and control of smart grids to be vulnerable to attacks, despite the fact that it is protected and it is represented using matrix Eq. (7).

$$E(s) = (M_c s)^{(-1)} + \begin{bmatrix} \frac{1}{0.1860+0.0006s} & \frac{-1}{0.1860+0.0006s} & 0 & 0 \\ \frac{-1}{0.1860+0.0006s} & \frac{1}{0.1860+0.0006s}+\frac{1}{0.1776+0.0005s} & \frac{-1}{0.1776+0.0005s} & 0 \\ 0 & \frac{-1}{0.1776+0.0005s} & \frac{1}{0.1776+0.0005s}+\frac{1}{0.2325+0.0007s} & \frac{1}{0.2325+0.0007s} \\ 0 & 0 & \frac{1}{0.2325+0.0007s} & \frac{1}{0.2325+0.0007s}+\frac{1}{12.3512+0.0152s} \end{bmatrix} \quad (7)$$

The attacks that were planned involve quantization, which is carried out by a uniform quantizer to extract the bit sequence $r(k)$ from measurements. This process aims to construct a dependable communication system. The RSC code is proposed to incorporate parity bits into the bit sequence. Generally, the RSC code is characterized by three parameters: the length of the codeword, denoted by n, the length of the message, denoted by m, and the length of the constraint, denoted by l, which is written as (n, m, l). When referring to the code rate, which indicates the number of parity bits added to the data stream, the quantity $\frac{1}{n}\frac{l}{n}$ is known as the code rate and is calculated using Eq. (7).

There are m-1 memory elements that are specified by the constraint length. These memory elements reflect the number of bits in the encoder memory that have an effect on the RSC generation output bits. Whenever the constraint length m is increased, the encoding process will inherently require more time in order to carry out the logical operations. There are additional benefits associated with the RSC code in comparison to the convolutional and turbo encoders. These benefits include a lower computation complexity, systematic output features, and the absence of an error floor [28]. When seen from this perspective, the RSC code (2, 1, 4) and the code generator polynomial (1 1 0 1, 1 1 1 1) are both taken into consideration in this study about the feedback process. In Figure 3, the first generator polynomial is located in the lower row, and the second polynomial is located in the upper row of the diagram. Therefore, the code rate is half of the normal rate, and the RSC process, which is where the logical operations are carried out, consists of three memories.

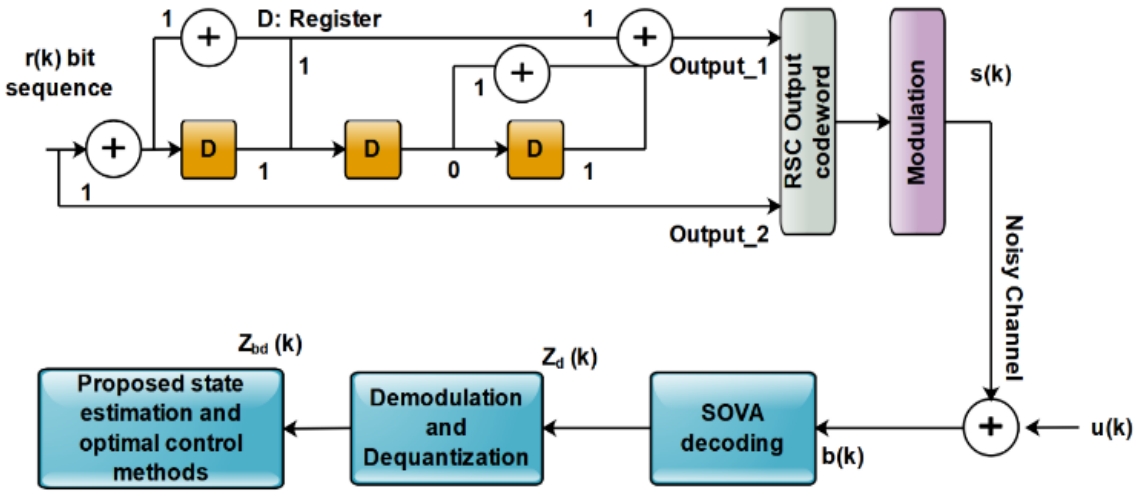

Figure 3. The RSC encoding procedure is used to protect against the cyber-attack

The RSC procedure is responsible for obtaining the codeword, which is then applied to the modulation in order to be transmitted. After being modulated, the signal *s(k)* is transmitted across a channel that is noisy. This is the signal that was received at the EMS is determine by using Eq. (8).

$$b(k) = s(k) + u(k) \quad (8)$$

where, $u(k)$ represents the additive white Gaussian noise in this context. The decoding step is then carried out using the soft output Viterbi algorithm (SOVA), which comes after the $b(k)$. In order to determine the maximum likelihood, estimate for the code sequence based on the signals that have been received, the SOVA algorithm is utilized. This particular method travels across the entirety of the trellis and then traces

back along the path with the highest likelihood, taking note of all of the path metrics [37-39]. The output $z_d(k)$ that has been decoded is then transferred to the module that is responsible for demodulation and de-quantization, and it is ultimately utilized for the purpose of state estimate.

Our proposed system, the Renewable Energy Smart Grid Protector and Controller (ReSGPC), integrates several components to enhance the security, efficiency, and reliability of smart grids. The primary components include:

4.1 Machine learning-based fault detection module

This module employs advanced machine learning algorithms to detect noise faults, cyberattacks, and signal attenuation in real-time. The primary machine learning techniques used are Long Short-Term Memory (LSTM) networks, Autoencoder LSTM (AE-LSTM), and Bidirectional LSTM (Bi-LSTM) [40].

(1) Kalman filter-based state estimation

Kalman filters are utilized to estimate the system state accurately. This component continuously monitors the grid's operational parameters and updates the state estimates, providing real-time data for decision-making [41-43].

(2) Optimal control law module

An optimal control law is developed to ensure the stability of the power network. This module uses the state estimates provided by the Kalman filter to regulate the power flow and maintain grid stability [44].

(3) Cybersecurity layer

The system incorporates a Recursive Systematic Convolutional (RSC) code to protect the communication infrastructure. This layer ensures the integrity and security of data transmitted across the grid [45].

4.2 Interaction of components

(1) Data collection and preprocessing

Sensors distributed across the grid collect real-time data, including voltage, current, and frequency measurements. This data is pre-processed to remove noise and outliers before being fed into the machine learning-based fault detection module [46].

(2) Fault detection and diagnosis

The preprocessed data is analyzed using LSTM, AE-LSTM, and Bi-LSTM networks. These models are trained to recognize patterns indicative of faults, cyberattacks, and signal attenuation. When an anomaly is detected, the system triggers an alert and provides diagnostic information [47-52].

(3) State estimation

The data, along with the fault detection results, is fed into the Kalman filter-based state estimation module. This module combines the real-time measurements with a mathematical model of the grid to estimate the current state of the system accurately [53].

(4) Control decision making

The state estimates are used by the optimal control law module to make real-time control decisions. The control law aims to optimize the performance index for grid control, ensuring efficient power distribution and minimizing losses [54].

(5) Communication security

The data transmitted between different components of the system is protected using RSC codes. This ensures that any attempt to tamper with the data is detected and mitigated, preserving the integrity of the control actions [55, 56].

4.3 Machine learning techniques employed

(1) Long short-term memory (LSTM) networks

LSTM networks are used for their ability to capture temporal dependencies in time-series data. They are particularly effective in detecting patterns that span over long sequences, making them ideal for identifying faults and cyberattacks in the grid [57-59].

(2) Autoencoder LSTM (AE-LSTM)

AE-LSTM is employed for its capability to learn compressed representations of the input data and detect anomalies. The autoencoder architecture helps in reconstructing the input data and identifying deviations that indicate potential issues.

(3) Bidirectional LSTM (Bi-LSTM)

Bi-LSTM networks process data in both forward and backward directions, providing a comprehensive understanding of the temporal dependencies. This enhances the accuracy of fault detection and diagnosis [60-63].

By integrating these components and machine learning techniques, the proposed ReSGPC system provides a robust solution for smart grid protection and control. The interaction between the fault detection module, state estimation, optimal control law, and cybersecurity layer ensures that the grid operates efficiently and securely, even in the presence of faults and cyber threats [64].

5. A PROPOSED FRAMEWORK FOR ESTIMATING AND CONTROLLING

The evaluation of the condition of the smart grid is an essential component in the process of controlling the operation of electricity networks [65-69]. Generally speaking, the expression Eq. (9) is that is used to express the expected system state estimate for the systems is (3) and (5):

$$\hat{y} - (k) = Q_d \hat{y}(k-1) + R_d j(k-1) \tag{9}$$

The value of $\hat{y}(k-1)$ represents the estimated state of the step that came before it. Consequently, the projected error covariance matrix can be expressed as Eq. (10):

$$H - (k) = Q_d H(k-1) Q_d^{\tau} + O_n(k-1) \tag{10}$$

The estimated error covariance matrix of the preceding step is denoted by the symbol $H(k-1)$ in this context. The Eq. (11) expresses the observation innovation residual $d(k)$:

$$d(k) = z_{bd}(k) - C\hat{y}(k) \tag{11}$$

where, $z_{bd}(k)$ represents the output sequence after it has been demodulated and dequantized. One way to express the Kalman

gain matrix is given in Eq. (12):

$$K(k) = H - (k)C^{\tau}[CH - (k)C^{\tau} + B_{\omega}(k)]^{-1} \quad (12)$$

Presented below is the most recent estimation of the state is given in Eq. (13):

$$\hat{y}(k) = \hat{y} - (k) + K(k)d(k) \quad (13)$$

After everything is said and done, the revised estimate error covariance matrix P(k) is calculated by using Eq. (14):

$$H(k) = H - (k) - K(k)CH - (k) \quad (14)$$

Following an estimation of the current state of the system, the control strategy that was proposed is implemented in order to regulate the system states.

The simulation result that will be presented in the following section demonstrates that the proposed estimation technique is capable of providing an accurate estimation of the state of the system. Therefore, in accordance with the separation principle [31-38]. it able to implement the control law $j(k) = Gy(k)$ [39-45], where F can be derived by solving the state feedback problem that is shown Eq. (15) [70-72].

$$j(k) = Gy(k) \quad (15)$$

To get the lowest possible value of the objective function is represented in Eq. (16):

$$Z = \sum_{k=0}^{\infty} [y'(k)O_{\aleph}y(k) + j'(k)B_{\aleph}j(k)] \quad (16)$$

A positive-definite state weighting matrix and a control weighting matrix are denoted by $O_{\aleph}$and $B_{\aleph}$, respectively, in this context [53-59]. F represents the state feedback gain matrix. Using the conventional trace operator and the Eq. (14), the Eq. (15) can be represented using Eq. (16) and Eq. (17). The Eq. (18) Eq. (19) and Eq.(20) is represented the standard format of equation of Eqs. (17) and (18) respectively [66].

$$Z = \sum_{K=0}^{\infty} \tau b[O_{\aleph} + G'B_{\aleph}G]H \quad (17)$$

$$H = (Q_d + R_dG)H(Q_d + R_d) \quad (18)$$

$$(Q_d + R_dG)HH^{-1}H(Q_d + R_dG)' - H + y(0)y'(0) \leq 0 \quad (19)$$

$$(Q_dH + R_dL)H^{-1}(Q_dH + R_dL)' - H + y(0)y'(0) \leq 0 \quad (20)$$

The Eq. (21) can be changed into the following form, according to Schur's complement, which is as follows:

$$\begin{bmatrix} y(0)y'(0) - H & Q_dH + R_dL \\ (Q_dH + R_dL)' & -H \end{bmatrix} \leq 0 \quad (21)$$

In the following, it will make an effort to locate a mild condition that guarantees the validity of Eq. (22) for any beginning condition *x(0)*. This will allow us to avoid the necessity of repeating the optimization technique for each additional *x(0)*. By solving the following linear matrix inequality, it is possible to satisfy the condition that (22) is sufficient for any beginning value.

$$\begin{bmatrix} S & B_{\aleph}^{\frac{1}{2}}\tilde{L} \\ \tilde{L}'B_{\aleph}^{\frac{1}{2}} & \tilde{H} \end{bmatrix} > 0 \quad (22)$$

The proposed optimization issue can be phrased is represented using Eq. (23) as a final proposition [68].

$$\min_{\tilde{H},S,\tilde{L}} \tau b[O_{\aleph}\tilde{H}] \quad (23)$$

The following is the calculation for the feedback gain matrix that has been proposed using Eq. (24).

$$G = \tilde{L}\widetilde{H^{-1}} \quad (24)$$

6. EXPERIMENTAL RESULTS AND DISCUSSION

Table 1 contains the parameters of the system. In addition, the cyber assault pattern that is being evaluated is comparable to the model that is presented in.

Table 1. The specifications of the system for the information security problem with the smart grid

Particulars	Values	Particular	Values
$O_{\aleph}$	$dig\ (10^{-2}, 10^{-2}, 10^{1}, 10^{-3})$	$B_{\aleph}$	$0.02*I_4$
Codes generator	$(14/15)_{octal}$	$\Delta\tau$	0.0002
Code rate	½	Channel	AWGA
Quantization	Uniform 16 bits	Decoding	SOVA
O_n	$0.0002*I_4$	B_{ω}	$0.001*I_4$

6.1 Software platform

The simulations were conducted using MATLAB, a high-level language and interactive environment for numerical computation, visualization, and programming. MATLAB is widely used for designing and simulating control systems due to its robust toolboxes and comprehensive mathematical functions.

6.2 Simulation duration

The simulation was run for a duration sufficient to capture the dynamic behavior and performance of the proposed smart grid protection and control system. Each simulation scenario was executed for a total of 1000 time steps, allowing for a thorough analysis of the system's response to various disturbances and operational conditions.

6.3 Assumptions made

Several assumptions were made to simplify the simulation and focus on the key aspects of the proposed method:

(1) Grid model

The smart grid was modeled as an IEEE 4-bus system with four distributed energy resources (DERs), specifically solar

panels, connected via inverters. The grid parameters were based on typical specifications for such systems.

(2) Initial conditions

The initial state values for the grid and DERs were assumed to be at nominal operating points. This assumption ensures that the system starts from a stable operating condition.

(3) Noise characteristics

The process noise $nd(k)$ and measurement noise $\omega(k)$ were assumed to be zero-mean Gaussian noise with known covariance matrices. This assumption is standard in Kalman filter-based estimation techniques.

(4) Communication infrastructure

The communication links between sensors, controllers, and the Energy Management System (EMS) were assumed to be secure but susceptible to cyber-attacks. Recursive Systematic Convolutional (RSC) codes were used to protect the transmitted data.

(5) Cyber-Attacks

The simulation included scenarios where the grid was subjected to cyber-attacks in the form of false data injection. These attacks aimed to alter the state measurements received by the EMS.

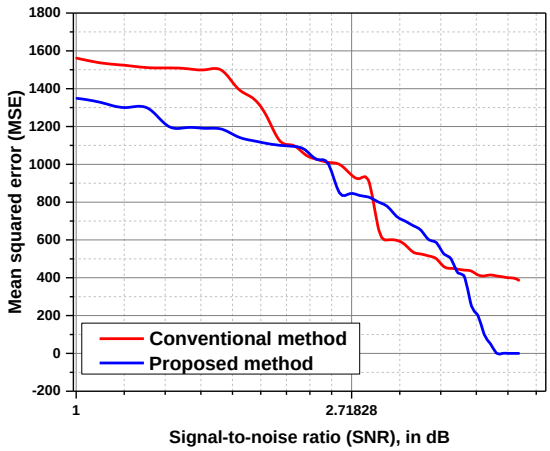

Figure 4. A comparison of the proposed method with the existing one using MSE and SNR analysis

To evaluate the performance, the mean squared error (MSE) between the actual state and the estimated state is used as the basis for comparison. In the first place, the mean square error (MSE) is compared to the signal-to-noise ratio (SNR) in Figure 3. When compared to the technique that is currently being used, it is clear that the estimator that has been provided offers superior performance [69]. it is because the RSC code is able to protect impairments, which is the reason for its success. In addition to this, SOVA has the capability of removing sounds from the signal that is received. In the second place, the results of the system state versus the time step are displayed in Figure 4 shows a comparison of the proposed method with the existing one using MSE and SNR analysis. It may be observed that the estimator delivers a performance that is satisfactory. Another thing that might be observed is that attacks have the potential to make the estimation of the system's state less accurate. Inaccurate estimates of system states generated by the currently available approach have the potential to directly mislead utility engineers, preventing them from conducting appropriate remedial control measures and dispatch decisions, which can ultimately result in a series of power outages. To put it another way, the communication infrastructure and estimate technique that has been provided would be an excellent choice for defending against cyber-attacks and providing real-time communication in both directions. Additionally, the design control law is implemented in the third place.

Figures 5-8 show the performance analysis actual state and predicted data obtained by proposed method with respect to the Δ_1, Δ_2, Δ_3, and Δ_4 respectively.

Figure 9 illustrates the performance analysis of the proposed method compared to existing methods in terms of efficiency, measured using the Mean Squared Error (MSE). Efficiency, in this context, refers to the system's ability to optimize resource usage, minimize energy losses, and maximize overall grid performance. The graph compares the MSE values for different scenarios or conditions, denoted as Δ1, Δ2, Δ3, and Δ4. Lower MSE values indicate better performance. The proposed method consistently shows lower MSE values across all scenarios, demonstrating superior efficiency in managing and controlling the smart grid compared to existing methods.

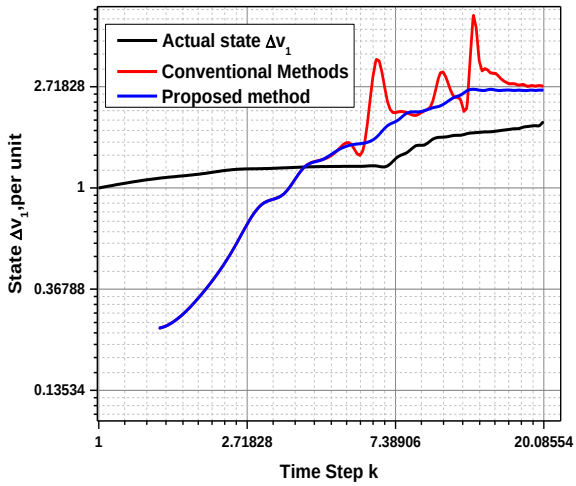

Figure 5. The performance analysis actual state and predicted data obtained by proposed method with respect to the Δ1

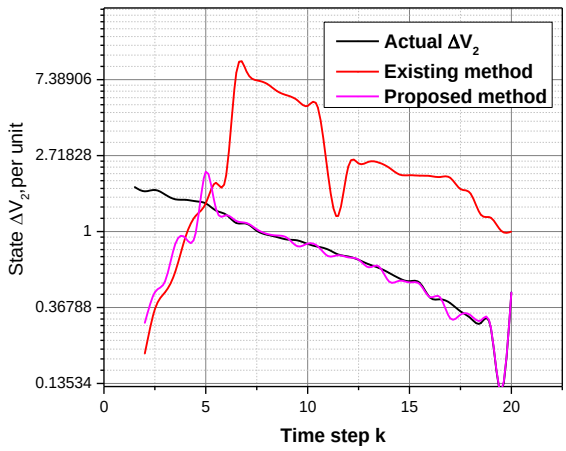

Figure 6. The performance analysis actual state and predicted data obtained by proposed method with respect to the Δ2

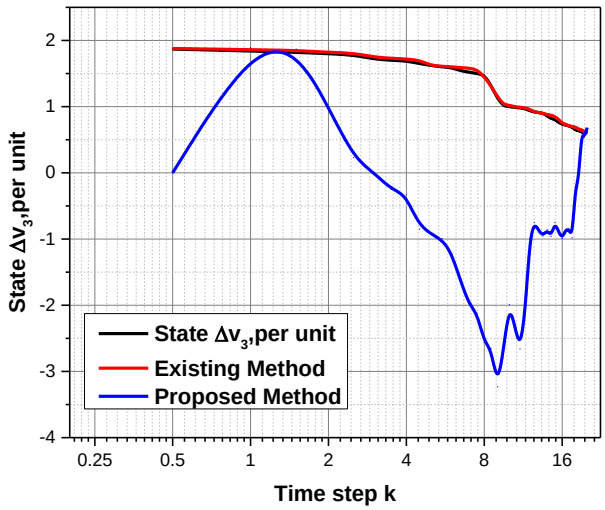

Figure 7. The performance analysis actual state and predicted data obtained by proposed method with respect to the Δ3

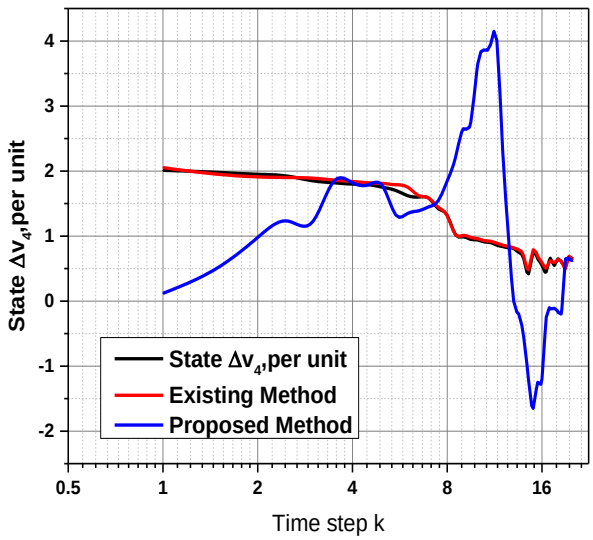

Figure 8. The performance analysis actual state and predicted data obtained by proposed method with respect to the Δ_4

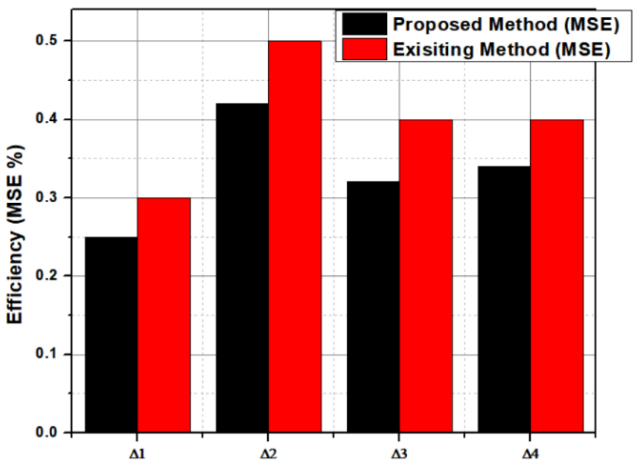

Figure 9. Performance analysis with respect to efficiency (MSE)

Figure 10 presents the performance analysis of the proposed method versus existing methods regarding stability and security. Stability is evaluated based on the system's ability to maintain steady and reliable operation under varying conditions, including load changes and disturbances. Security measures the system's ability to protect against cyber threats and ensure data integrity. The graph compares the MSE values for stability and security metrics under different scenarios (Δ1, Δ2, Δ3, Δ4). Lower MSE values indicate better stability and security. The proposed method demonstrates significantly lower MSE values, highlighting its enhanced stability and robust security features compared to existing methods.

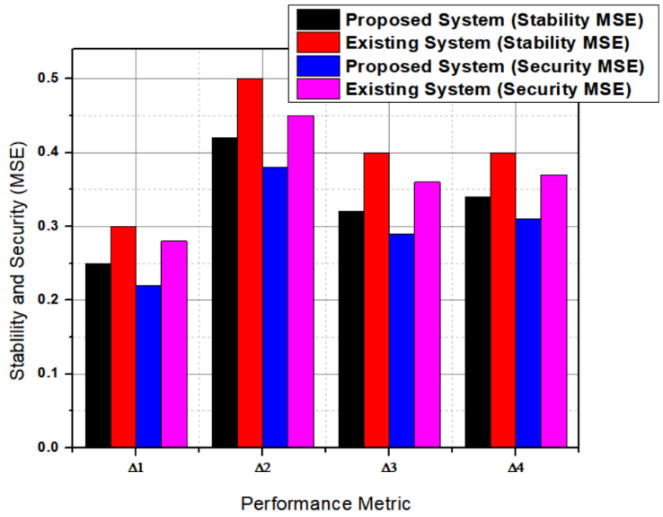

Figure 10. Performance analysis with respect to stability and security

7. CONCLUSION

This paper focuses mainly on smart grid protection and control using machine-learning-based power management systems. The proposed method is capable of handling cyberattacks, attenuations, faulty systems, and effectively controlling. In addition to this, the performance of the proposed approach in comparison to the performance of conventional ways has resulted in an increase in the efficiency which the smart grid possesses. The additional layer of protection that the proposed approach offers to the code for the system that is responsible for protecting the grid information is provided by the proposed method. A control law that is optimal is developed by us in order to guarantee the reliability of the power network. Within the framework of a convex semidefinite programming exercise, the work carry out conversion by focusing primarily on the performance index for control. The controller is capable of performing all of its functions properly, regardless of the beginning values. Regardless of the numbers that were initially set, there is a significant improvement in the effectiveness of the controller. The developed method is validated through the use of numerical simulations. The results of this performance analysis of the strategy that was proposed demonstrate that the way that was advised provides a more effective line of attack. The smart grid is a dependable and system-based communication infrastructure that incorporates applications that integrate renewable resources. This technique provides a critical energy management framework for the smart grid. The

simulation analysis, considering five cases, demonstrates that the proposed method outperforms the conventional method in all cases. The proposed method has determined the improvement in performance of 0.25%, 0.42%, 0.32%, 0.25%, and 0.34% of MSE, Δ_1, Δ_2, Δ_3, and Δ_4 respectively.

8. FUTURE SCOPE

The integration of machine learning and Kalman filters into smart grid protection and control systems heralds a new era in power management. This approach promises enhanced accuracy in real-time prediction and optimization of grid performance, ensuring stability and efficiency. The adaptive nature of machine learning algorithms, combined with the precision of Kalman filters in estimating system states, allows for more effective management of dynamic grid conditions. This includes better fault detection, predictive maintenance, and load balancing. Future developments could see these systems being increasingly autonomous, capable of self-healing and adapting to evolving energy demands and generation patterns. Integration with renewable energy sources and storage systems will be key, as will the ability to withstand and quickly recover from cyber and physical threats. The role of these advanced systems in facilitating smart cities and IoT applications is also significant, offering a more sustainable and resilient energy future.

ACKNOWLEDGMENT

The authors would like to thank SJB Institute of Technology, JSS Academy of Technical Education, Bengaluru, Visvesvaraya Technological University (VTU), Belagavi and Vision Group on Science and Technology (VGST) Karnataka Fund for Infrastructure strengthening in Science & Technology Level-2 sponsored "Establishment of Renewable Smart Grid Laboratory" for all the support and encouragement provided by them to take up this research work and publish this paper.

REFERENCES

[1] Le, R., Wang, X. (2018). Smart power grid synchronization using extended Kalman filtering: Theory and implementation with CompactRIO. In 2018 IEEE Green Technologies Conference (GreenTech), Austin, TX, USA, pp. 38-43. https://doi.org/10.1109/GreenTech.2018.00016

[2] Luo, X., Bai, M., Wang, X., Sun, X. (2021). Square-root extended kalman filter-based detection of false data injection attack in smart grids. In 2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2), Taiyuan, China, pp. 2376-2381. https://doi.org/10.1109/EI252483.2021.9713070

[3] Thazeen, S., Mallikarjunaswamy, S., Saqhib, M.N., Sharmila, N. (2022). DOA method with reduced bias and side lobe suppression. In 2022 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, pp. 1-6. https://doi.org/10.1109/IC3IOT53935.2022.9767996

[4] Dayananda, P., Srikantaswamy, M., Nagaraju, S., Velluri, R., Kumar, D.M. (2022). Efficient detection of faults and false data injection attacks in smart grid using a reconfigurable Kalman filter. International Journal of Power Electronics and Drive Systems (IJPEDS), 13(4): 2086-2097. https://doi.org/10.11591/ijpeds.v13.i4.pp2086-2097

[5] Mahendra, H.N., Mallikarjunaswamy, S., Subramoniam, S.R. (2023). An assessment of vegetation cover of Mysuru City, Karnataka State, India, using deep convolutional neural networks. Environmental Monitoring and Assessment, 195(4): 526. https://doi.org/10.1007/s10661-023-11140-w

[6] Rana, M.M., Bo, R., Choi, B.J. (2019). Residual saturation based Kalman filter for smart grid state estimation under cyber attacks. In 2019 IEEE 9th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Suzhou, China, pp. 1459-1463. https://doi.org/10.1109/CYBER46603.2019.9066737

[7] Sawodny, J., Riedel, O., Namerikawa, T. (2020). Detection of attacks in smart grids via extended Kalman filter and correlation analysis. In 2020 59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), Chiang Mai, Thailand, IEEE, pp. 663-669. https://doi.org/10.23919/SICE48898.2020.9240229

[8] Swain, S., Subudhi, B. (2018). Grid synchronization of a PV system with power quality disturbances using unscented Kalman filtering. IEEE Transactions on Sustainable Energy, 10(3): 1240-1247. https://doi.org/10.1109/TSTE.2018.2864822

[9] Akbarian, F., Ramezani, A., Hamidi-Beheshti, M.T., Haghighat, V. (2018). Intrusion detection on critical smart grid infrastructure. In 2018 Smart Grid Conference (SGC), Sanandaj, Iran, pp. 1-6. https://doi.org/10.1109/SGC.2018.8777815

[10] Mallikarjunaswamy, S., Nataraj, K.R., Rekha, K.R. (2014). Design of high-speed reconfigurable coprocessor for next-generation communication platform. In Emerging Research in Electronics, Computer Science and Technology: Proceedings of International Conference, ICERECT 2012, Springer India, pp. 57-67. https://doi.org/10.1007/978-81-322-1157-0_7

[11] Zhang, R., Zhang, Q., Wang, Z., Sun, H. (2021). Detection of false data injection attack in smart grid based on iterative Kalman filter. In 2021 China Automation Congress (CAC), Beijing, China, pp. 6083-6088. https://doi.org/10.1109/CAC53003.2021.9728537

[12] Liu, Y., Cheng, L. (2022). Relentless false data injection attacks against Kalman-filter-based detection in smart grid. IEEE Transactions on Control of Network Systems, 9(3): 1238-1250. https://doi.org/10.1109/TCNS.2022.3141026

[13] Jin, S., Yang, X., Wang, C., Wang, S., Store, D.I. (2023). A novel robust back propagation neural networkdual extended Kalman filter model for state-ofcharge and state-of-health co-estimation of lithiumion batteries. In 2023 IEEE PES Conference on Innovative Smart Grid Technologies-Middle East (ISGT Middle East), Abu Dhabi, United Arab Emirates, pp. 1-5. https://doi.org/10.1109/ISGTMiddleEast56437.2023.10078467

[14] Shair, J., Wu, C., Huang, W., Xie, X. (2019). Extracting time-varying subsynchronous oscillation in wind power systems through kalman filtering. In 2019 IEEE

Innovative Smart Grid Technologies-Asia (ISGT Asia), Chengdu, China, pp. 3162-316. https://doi.org/10.1109/ISGT-Asia.2019.8881473
[15] Sahu, S., Dutt, R., Acharyya, A. (2023). Battery states co-estimation methodology using dual square root unscented kalman filter. In 2023 IEEE International Symposium on Circuits and Systems (ISCAS), Monterey, CA, USA, pp. 1-5. https://doi.org/10.1109/ISCAS46773.2023.10181678
[16] Rashed, M., Kamruzzaman, J., Gondal, I., Islam, S. (2022). False data detection in a clustered smart grid using unscented Kalman filter. IEEE Access, 10: 78548-78556. https://doi.org/10.1109/ACCESS.2022.3193781
[17] Rana, M.M., Li, L. (2015). Distributed generation monitoring of smart grid using accuracy dependent Kalman filter with communication systems. In 2015 12th International Conference on Information Technology-New Generations, Las Vegas, NV, USA, pp. 496-500. https://doi.org/10.1109/ITNG.2015.154
[18] Wang, Y., Zhang, Z., Ma, J., Jin, Q. (2021). KFRNN: An effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network. IEEE Internet of Things Journal, 9(9): 6893-6904. https://doi.org/10.1109/JIOT.2021.3113900
[19] Alqahtani, N., Ganesan, S., Zohdy, M., Olawoyin, R. (2020). Optimal asynchrophasor in PMU using second order kalman filter. In 2020 IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, pp. 635-637. https://doi.org/10.1109/EIT48999.2020.9208286
[20] Li, Y., He, X., Zhang, W. (2014). Applications of adaptive CKF algorithm in short-term load forecasting of smart grid. In Proceedings of the 33rd Chinese Control Conference, Nanjing, China, pp. 8145-8149. https://doi.org/10.1109/ChiCC.2014.6896364
[21] Dutt, R., Chodisetti, M., Acharyya, A. (2020). Real-time and accurate state-of-charge estimation methodology using dual square root unscented kalman filter. In 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Seville, Spain, pp. 1-5. https://doi.org/10.1109/ISCAS45731.2020.9181049
[22] De, S., Sodhi, R. (2020). A simple cyber attack detection scheme for smart grid cyber security enhancement. In 2020 21st National Power Systems Conference (NPSC), Gandhinagar, India, pp. 1-6. https://doi.org/10.1109/NPSC49263.2020.9331837
[23] Guo, X., Tang, M., Li, J., An, B. (2023). Optimization study of electric vehicle charging station load model prediction based on Kalman filtering. In 2023 7th International Conference on Smart Grid and Smart Cities (ICSGSC), Lanzhou, China, pp. 456-461. https://doi.org/10.1109/ICSGSC59580.2023.10318964
[24] Pei, C., Xiao, Y., Liang, W., Han, X. (2021). A deviation-based detection method against false data injection attacks in smart grid. IEEE Access, 9: 15499-15509. https://doi.org/10.1109/ACCESS.2021.3051155
[25] Karimi, H.S., Natarajan, B. (2020). Recursive dynamic compressive sensing in smart distribution systems. In 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, pp. 1-5. https://doi.org/10.1109/ISGT45199.2020.9087784
[26] Li, J., Zhang, Y. (2022). UKF-based state estimation for smart grids under false data injection attacks. In 2022 IEEE Electrical Power and Energy Conference (EPEC), Victoria, BC, Canada, pp. 374-379. https://doi.org/10.1109/EPEC56903.2022.10000114
[27] Liu, Y., Xue, W., He, S., Cheng, L. (2021). Stealthy false data injection attacks against extended Kalman filter detection in power grids. In 2021 8th International Conference on Information, Cybernetics, and Computational Social Systems (ICCSS), Beijing, China, pp. 459-464. https://doi.org/10.1109/ICCSS53909.2021.9721954
[28] Liu, X., Li, L., Li, Z., Chen, X., Fernando, T., Iu, H.H.C., He, G. (2017). Event-trigger particle filter for smart grids with limited communication bandwidth infrastructure. IEEE Transactions on Smart Grid, 9(6): 6918-6928. https://doi.org/10.1109/TSG.2017.2728687
[29] Xiao, J., Wang, L., Qin, Z., Bauer, P. (2022). Detection of cyber attack in smart grid: A comparative study. In 2022 IEEE 20th International Power Electronics and Motion Control Conference (PEMC), Brasov, Romania, pp. 48-54. https://doi.org/10.1109/PEMC51159.2022.9962902
[30] Frisch, D., Hanebeck, U.D. (2021). Deterministic gaussian sampling with generalized fibonacci grids. In 2021 IEEE 24th International Conference on Information Fusion (FUSION), Sun City, South Africa, pp. 1-8. https://doi.org/10.23919/FUSION49465.2021.9626975
[31] Wu, Y., Zhou, D. (2021). Simulation research and embedded implementation of model based soc estimation for lithium battery. In 2021 6th International Conference on Smart Grid and Electrical Automation (ICSGEA), Kunming, China, pp. 125-129. https://doi.org/10.1109/ICSGEA53208.2021.00033
[32] Mohammadrezaee, R., Ghaisari, J., Yousefi, G., Kamali, M. (2021). Dynamic state estimation of smart distribution grids using compressed measurements. IEEE Transactions on Smart Grid, 12(5): 4535-4542. https://doi.org/10.1109/TSG.2021.3071514
[33] Sheta, A.N., Abdulsalam, G.M., Sedhom, B.E., Eladl, A.A. (2023). Comparative framework for AC-microgrid protection schemes: Challenges, solutions, real applications, and future trends. Protection and Control of Modern Power Systems, 8(2): 1-40. https://doi.org/10.1186/s41601-023-00296-9
[34] Mahendra, H.N., Mallikarjunaswamy, S., Kumar, D.M., Kumari, S., Kashyap, S., Fulwani, S., Chatterjee, A. (2023). Assessment and prediction of air quality level using ARIMA model: A case study of surat city, Gujarat State, India. Nature Environment & Pollution Technology, 22(1): 199-210. https://doi.org/10.46488/NEPT.2023.v22i01.018
[35] Chao, W., Dai, L., Huang, J., Chen, M. (2023). Research on hybrid active power filter and its control and protection system for LCC-HVDC. In 2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 2023, pp. 139-142. https://doi.org/10.1109/ITAIC58329.2023.10408866
[36] Mahendra, H.N., Mallikarjunaswamy, S., Subramoniam, S.R. (2023). An assessment of built-up cover using geospatial techniques-a case study on Mysuru District, Karnataka State, India. International Journal of Environmental Technology and Management, 26(3-5): 173-188. https://doi.org/10.1504/IJETM.2023.130787
[37] Pooja, S., Mallikarjunaswamy, M., Sharmila, S. (2023).

Image region driven prior selection for image deblurring. Multimedia Tools and Applications, 82: 24181-24202. https://doi.org/10.1007/s11042-023-14335-y

[38] Yan, L., Li, D., Liang, H., Li, S. (2023). Design of power grid cloud security terminal protection system based on level protection. In 2023 2nd International Conference on Smart Grids and Energy Systems (SGES), Guangzhou, China, 2023, pp. 86-90. https://doi.org/10.1109/SGES59720.2023.10366944

[39] Mallikarjunaswamy, S., Basavaraju, N.M., Sharmila, N., Mahendra, H.N., Pooja, S., Deepak, B.L. (2022). An efficient big data gathering in wireless sensor network using reconfigurable node distribution algorithm. In 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), Bengaluru, India, pp. 1-6. http://doi.org/10.1109/CCIP57447.2022.10058620

[40] Mahendra, H.N., Mallikarjunaswamy, S. (2022). An efficient classification of hyperspectral remotely sensed data using support vector machine. International Journal of Electronics and Telecommunications, 68(3): 609-617. http://doi.org/10.24425/ijet.2022.141280

[41] Shivaji, R., Nataraj, K.R., Mallikarjunaswamy, S., Rekha, K.R. (2022). Implementation of an effective hybrid partial transmit sequence model for peak to average power ratio in MIMO OFDM system. In ICDSMLA 2020: Proceedings of the 2nd International Conference on Data Science, Machine Learning and Applications. Springer Singapore, 783: 1343-1353. https://doi.org/10.1007/978-981-16-3690-5_129

[42] Kumar, R., Batra, R., Ezhilarasan, G. (2023). Safe communication system implementation in in smart grids with the hybrid systems. In 2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC), Greater Noida, India, pp. 1380-1384. https://doi.org/10.1109/PEEIC59336.2023.10450840

[43] Venkatesh, D.Y., Mallikarjunaiah, K., Srikantaswamy, M. (2022). A comprehensive review of low density parity check encoder techniques. Ingénierie des Systemes d'Information, 27(1): 11-20. https://doi.org/10.18280/isi.270102

[44] Tefek, U., Esiner, E., Cheh, C., Mashima, D. (2023). A smart grid ontology: Vulnerabilities, attacks, and security policies. In 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA, pp. 1-6. https://doi.org/10.1109/CNS59707.2023.10289085

[45] Mahendra, H.N., Mallikarjunaswamy, S., Basavaraju, N.M., Poojary, P.M., Gowda, P.S., Mukunda, M., Navya, B., Pushpalatha, V. (2022). Deep learning models for inventory of agriculture crops and yield production using satellite images. In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, pp. 1-7. https://doi.org/10.1109/MysuruCon55714.2022.9972523

[46] Mahendra, H.N., Mallikarjunaswamy, S., Nooli, C.B., Hrishikesh, M., Kruthik, N., Vakkalanka, H.M. (2022). Cloud based centralized smart cart and contactless billing system. In 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, pp. 820-826. https://doi.org/10.1109/ICCES54183.2022.9835856

[47] Mallikarjunaswamy, S., Sharmila, N., Siddesh, G.K., Nataraj, K.R., Komala, M. (2022). A novel architecture for cluster based false data injection attack detection and location identification in smart grid. In Advances in Thermofluids and Renewable Energy: Select Proceedings of TFRE 2020. Springer Singapore, pp. 599-611. https://doi.org/10.1007/978-981-16-3497-0_48

[48] Thazeen, S., Mallikarjunaswamy, S., Siddesh, G.K., Sharmila, N. (2021). Conventional and subspace algorithms for mobile source detection and radiation formation. Traitement du Signal, 38(1): 135-145. https://doi.org/10.18280/ts.380114

[49] Satish, P., Srikantaswamy, M., Ramaswamy, N.K. (2020). A comprehensive review of blind deconvolution techniques for image deblurring. Traitement du Signal, 37(3): 527-539. https://doi.org/10.18280/ts.370321

[50] Kumar, S.M., Nagaraj, S., Veerabhadraswamy, P., Nanjundaswamy, M.H., Srikantaswamy, M., Chandratta, K.Y. (2024). An enhanced power management and prediction for smart grid using machine learning. In: Shukla, S., Sayama, H., Kureethara, J.V., Mishra, D.K. (eds) Data Science and Security. IDSCS 2023. Lecture Notes in Networks and Systems, vol 922. Springer, Singapore. https://doi.org/10.1007/978-981-97-0975-5_24

[51] Mahendra, H.N., Mallikarjunaswamy, S., Rekha, V., Puspalatha, V., Sharmila, N. (2019). Performance analysis of different classifier for remote sensing application. International Journal of Engineering and Advanced Technology, 9(1): 7153-7158. https://doi.org/10.35940/ijeat.A1879.109119

[52] Thazeen, S., Mallikarjunaswamy, S. (2023). The effectiveness of 6T beamformer algorithm in smart antenna systems for convergence analysis. IIUM Engineering Journal, 24(2): 100-116. https://doi.org/10.31436/iiumej.v24i2.2730

[53] Honnegowda, J., Mallikarjunaiah, K., Srikantaswamy, M. (2024). An efficient abnormal event detection system in video surveillance using deep learning-based reconfigurable autoencoder. Ingénierie des Systèmes d'Information, 29(2): 677-686. https://doi.org/10.18280/isi.290229

[54] Wang, W., Yorino, N., Sasaki, Y., Zoka, Y., Bedawy, A., Kawauchi, S. (2021). Adaptive model predictive-based load frequency controller using unscented kalman filter. In 2021 IEEE PES Innovative Smart Grid Technologies-Asia (ISGT Asia), Brisbane, Australia, pp. 1-5. https://doi.org/10.1109/ISGTAsia49270.2021.9715589

[55] Katić, V.A., Stanisavljević, A.M., Turović, R.L., Dumnić, B.P., Popadić, B.P. (2018). Extended kalman filter for voltage dips detection in grid with distributed energy resources. In 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, pp. 1-6. https://doi.org/10.1109/ISGTEurope.2018.8571857

[56] Sheela, S., Naveen, K.B., Basavaraju, N.M., Kumar, D.M., Krishnaiah, M., Mallikarjunaswamy, S. (2023). An efficient vehicle to vehicle communication system using intelligent transportation system. In 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), B G NAGARA, India, pp. 1-6. https://doi.org/10.1109/ICRASET59632.2023.10420043

[57] Rana, M.M., Abdelhadi, A., Bo, R. (2020). Distributed attack-resilient grid state estimation algorithm using optimal filter and graph theory. In 2020 IEEE

International Symposium on Systems Engineering (ISSE), Vienna, Austria, pp. 1-5. https://doi.org/10.1109/ISSE49799.2020.9272241

[58] Zhang, T., An, D. (2023). Data integrity attack strategy against state estimation results of distributed power system. In 2023 5th Asia Energy and Electrical Engineering Symposium (AEEES), Chengdu, China, pp. 1146-1151. https://doi.org/10.1109/AEEES56888.2023.10114340

[59] Kunac, A., Petrovic, G., Despalatovic, M., Sarajcev, P. (2022). Grid voltage amplitude and frequency real-time estimation using linear kalman filter. In 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), Split/Bol, Croatia, pp. 1-6. https://doi.org/10.23919/SpliTech55088.2022.9854381

[60] Kavya, B.M., Sharmila, N., Naveen, K.B., Mallikarjunaswamy, S., Manu, K.S., Manjunatha, S. (2023). A machine learning based smart grid for home power management using cloud-edge computing system. In 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), B G NAGARA, India, pp. 1-6. https://doi.org/10.1109/ICRASET59632.2023.10419952

[61] Feng, Y., Yang, D. (2019). Kalman filter-based centralized controller design for smart microgrid. In 2019 Chinese Automation Congress (CAC), Hangzhou, China, pp. 2185-2190. https://doi.org/10.1109/CAC48633.2019.8996930

[62] Zhao, J., Mili, L. (2018). A decentralized H-infinity unscented Kalman filter for dynamic state estimation against uncertainties. IEEE Transactions on Smart Grid, 10(5): 4870-4880. https://doi.org/10.1109/TSG.2018.2870327

[63] Chen, B., Wu, W., Gao, C., Orabi, M., Koutroulis, E., Chung, H., Blaabjerg, F. (2022). A new stability enhancement method using KF estimation for the PWM-SMC-based grid-tied inverter under weak grid condition. IEEE Journal of Emerging and Selected Topics in Power Electronics, 10(6): 6950-6959. https://doi.org/10.1109/JESTPE.2022.3178733

[64] Howard, M.D., Qu, Z. (2021). An optimal kalman-consensus filter for distributed implementation over a dynamic communication network. IEEE Access, 9: 66696-66706. https://doi.org/10.1109/ACCESS.2021.3076981

[65] Wang, H., Wen, X., Xu, Y., Zhou, B., Peng, J., Liu, W. (2020). Operating state reconstruction in cyber physical smart grid for automatic attack filtering. IEEE Transactions on Industrial Informatics, 18(5): 2909-2922. https://doi.org/10.1109/TII.2020.3000172

[66] Alsabilah, N., Rawat, D.B. (2021). Anomaly detection in smart home networks using Kalman filter. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, pp. 1-6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484507

[67] Kurt, M.N., Ogundijo, O., Li, C., Wang, X. (2018). Online cyber-attack detection in smart grid: A reinforcement learning approach. IEEE Transactions on Smart Grid, 10(5): 5174-5185. https://doi.org/10.1109/TSG.2018.2878570

[68] Shankara, K.H., Srikantaswamy, M., Nagaraju, S. (2024). A comprehensive study on DC-DC converter for equal current sharing and voltage stability in renewable energy resources. Journal Européen des Systèmes Automatisés, 57(2): 323-334. https://doi.org/10.18280/jesa.570202

[69] Assimakis, N., Manasis, C., Ktena, A. (2019). Electric load estimation using kalman and lainiotis filters. In 2019 8th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, pp. 1-4. https://doi.org/10.1109/MECO.2019.8760144

[70] Bhat, C., Herle, A., Channegowda, J., Naraharisetti, K. (2022). Battery parameter evaluation using unscented kalman filter for electric vehicle drive cycles. In 2022 IEEE International Conference on Power Electronics, Smart Grid, and Renewable Energy (PESGRE), Trivandrum, India, pp. 1-5. https://doi.org/10.1109/PESGRE52268.2022.9715919

[71] Manjunatha, S., Swetha, M.D., Rashmi, S., Subramanian, A.K. (2024). Convolutional neural network-based image tamper detection with Error Level Analysis. In 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bangalore, India, pp. 1-7. https://doi.org/10.1109/IITCEE59897.2024.10467563

[72] Kong, X., Zhang, X., Lu, N., Ma, Y., Li, Y. (2021). Online smart meter measurement error estimation based on EKF and LMRLS method. IEEE Transactions on Smart Grid, 12(5): 4269-4279. https://doi.org/10.1109/TSG.2021.3077693