Microsystem Technologies
https://doi.org/10.1007/s00542-023-05596-6

TECHNICAL PAPER

An island detection methodology with protection against cyber attack

Apoorva Shukla[1] · Soham Dutta[2] · Pradip Kumar Sadhu[1] · Bishwajit Dey[3]

Received: 9 March 2023 / Accepted: 18 December 2023

Abstract

Unplanned islanding of micro-grids is a significant barrier to supplying continuous power to key customers. The identification of the islanding moments must be rapid to enable the distributed generators (DG) to perform control measures in the shortest possible period. Micro phasor measuring units (μ-PMU) are gaining popularity in distribution systems and micro grids as a result of their ability to produce high-quality data at a high speed. These μ-PMUs can be utilized to detect islands. However, the μ-PMU relies heavily on the communication system for transmission of data, which is vulnerable to cyberattacks. In consideration of the previous technique, this research provides a smart island detection application with μ-PMU having lowered cyberattack probabilities. This representation is equipped with a μ-PMU implemented on the relevant DG's bus. The voltage data acquired from these μ-PMUs are processed using the sequence transformation in order to simulate the sequence component angle. The angular sum of the negative and positive sequence components is evaluated and the maximum value is deployed for detection of islanding. MATLAB/Simulink tests the proposed approach through an IEEE-34 node distribution network. Multiple simulations demonstrate the robustness of the technique.

1 Introduction

Smart grid has reinforced the foundation of today's society by competent generation and transmission of electricity to users across a vast topographical area. The primary goal of smart grid is to provide uninterrupted electricity to important consumers such as hospitals, emergency centres, factories, and transport systems (Ahmad et al. 2022), that implies continuous production. So, it is necessary to guarantee that these loads have a steady power supply. However, the expanding utilization of distributed generators (DG) in distribution systems poses a number of technical issues, including unintended islanding (Dey et al. 2023). The unintended islanding results in negative effects such as reclosing in out-of-phase, deteriorating quality of power, and concerns in safety for the maintenance staff, and so on (Shukla et al. 2023a). Therefore, the identification of the islanding events is required for the sustaining of essential loads under hostile conditions.

✉ Soham Dutta
soham.dutta@manipal.edu

1 Department of Electrical Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, Jharkhand 826004, India

2 Department of Electrical and Electronics Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka 576104, India

3 Department of Electrical Engineering, Adani University, Ahmedabad, Gujarat 382421, India

1.1 Motivation

As the information technology grabbed its foothold in the smart grid sector, cyberattacks have become increasingly prevalent in modern electrical grid, jeopardizing its reliability and resilience (Duo et al. 2022). Moreover, in an epoch of open markets, the likelihood of data mismanagement increases, provided that the approach is unprotected end-to-end. The present electrical energy system is a complex cyber-physical structure in which the both the physical as well as cyber layers are highly intertwined. The physical component consists of electrical along with mechanical structures and are accountable to electrical generation, transmission as well as distribution. Meanwhile, the cyber component consists of collecting data, processing it and then transmission of the data. As illustrated by Fig. 1, the modern smart grid consists of five primary components: the grid, the communication network, the sensor network, the controller network, and at last the actuator network. Important grid characteristics are measured by the sensor network, and the data measured is channelled to the control centre via the communication grid to process and implement the control actions (Dutta et al.

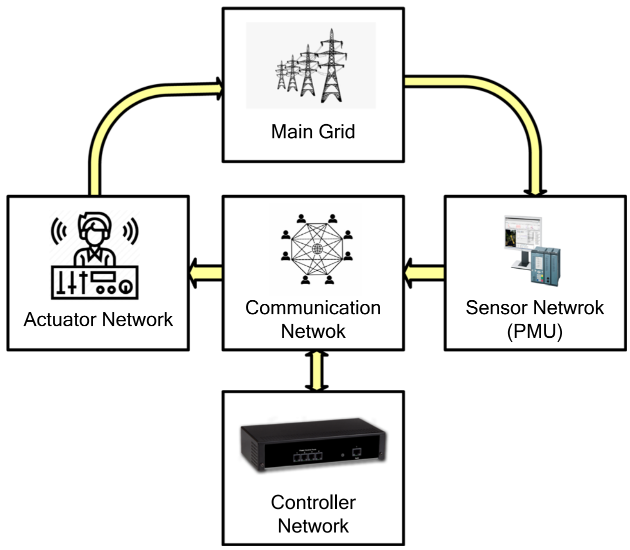

Fig. 1 Modern smart grid components

2023). These control actions are subsequently transmitted via the communication network to the network of actuators, which implements physical operations on the power. Cyber assailants target power system components that rely heavily on information technology, like sensor networks e.g. phasor measurement units (PMUs), smart meters, controller networks with programmable logics and the communication networks that rely on cables, diversified technologies, and arrangement for effective transfer of data (Dutta et al. 2022a). Consequently, the data communicated in the smart grid design concerning line flow, voltage measurement, power injection and state of breakers, switches, relays, etc., is susceptible to cyberattacks. In addition, as shown in Fig. 1, the attacks are recursive because of the interconnection of the various power system components. One strategy to lessen the likelihood of a cyberattack is to reducing the interdependence of these components of power system.

The micro-grid can function in either grid-connected or island mode. In islanded approach, a portion of the grid is detached from the main power grid system, while the DG existing in the disconnected-grid or micro-grid continues to supply power to the disconnected grid. Islanding might be intended or accidental. Generally, intended islanding is performed for repair and maintenance purposes. In intended islanding, since it is known ahead that the micro-grid would be islanded, it is simple to regulate the frequency and power of the islanded grid. In the event of accidental islanding, the linked DG of the islanded micro-grid must draw out itself within 2 s, by following IEEE Standard 1547-2018. This is important to prevent severe frequency and voltage imbalances in the islanded grid, consequently protecting electrical equipment from damage. Identification of accidental island situations is therefore required for the efficient operation of micro-grids. The island detection approach implicates monitoring some data in the micro-grid by using measurement device, delivering the data through a communication channel to a control centre, where it will be processed by software procedures, and finally send control indications across the same communication network to the relevant relays of the DG (Shukla et al. 2023b). Cyberattacks can interfere with this detection process in the manners listed below:

1. The attackers can initiate denial-of- service, introduce fake data, or they can destruct the communication network between the control centre and measuring device or the relays and control centre respectively.
2. If an attacker executes a fake island detection signal while there is no actual islanding situation, the micro-grid will have power loss erroneously, paving way for blackout in the region. It will decrease the micro-grid's dependability and resilience. The repair team of the micro-grid uninformed about the cables being still energized by the main grid, will experience significant shock. This could be lethal for them.
3. If an attacker defragments an actual islanding scenario, the micro-grid will experience significant frequency and voltage variations, which further degrades power quality and damages electrical equipment.
4. Before reconnecting the main grid and the islanded grid, the frequency in the islanded area must be stabilized and synchronized. If not, an enormous current will circulate, causing equipment damage. Attackers can damage the power grid by interrupting this situation.

In several regions around the world, the implementation of time-synchronized PMU has contributed to the enhancement of the smart grid's dependability. To transmit phasor data within milliseconds, PMUs utilize data networks with many gateways among phasor data concentrators (PDC), control centres, measurement sites, and super PDC (De and Sodhi 2022). This has led to a rise in cyberattacks. The hackers can tamper with the cables manually, perform denial-of-service threats through network traffic hindrance, or insert fake PMU packets of data. In addition to replacing the actual data with the fake data, the attackers can also rephrase the data. As PMUs utilize Global Positioning System (GPS) signals, it is possible for attackers to block or forge these signals. Rapid spread of distributed networks across a large geographical area has led to widespread use of micro phasor measurement units (μ-PMUs) for dynamic monitoring, state estimates, etc. The μ-PMU measures data at an extremely fast pace and with a great degree of precision (Dutta et al. 2020; Mirshekali et al. 2022). Consequently, these can be used for island detection. Avoiding the data stream is one technique to protect the island detecting algorithm from cyber threats. This involves processing the large amount of information within the µ-PMU using an appropriate technique for signal analysis. In order to reduce reliance on the information transmission network, an intelligent µ-PMU that performs measurements and makes key decisions using signal processing is required.

1.2 Related work

Many strategies of islanding detection have been published in research publications, that is generally segregated as active (Bahrani et al. 2009), passive (Ashour et al. 2013), local, hybrid (Larik et al. 2022), signal processing (Raza et al. 2015), and intelligence-based islanding detection (Ahmad et al. 2013). With passive approaches, grid parameters are continuously monitored, and islanding is identified when the parameter value exceeds a predefined threshold. Some of the most recent passive strategies are based on enhanced voltage shift (Liu et al. 2016), derivative of equivalent resistance with respect to time index (Xie et al. 2020), active rate of change of frequency (ROCOF) relay (Gupta et al. 2016), voltage index (Abd-Elkader et al. 2018), variational mode decomposition based mode singular entropy (Admasie et al. 2019), harmonic distortion, over/under frequency and voltage, rate of change of power, phase jump detection, etc. (Dutta et al. 2022b; Freitas et at. 2005; Redfern et al. 1993; Mishra et al. 2019). Simple, but with a huge non detection zone (NDZ) characterize the passive islanding techniques (Zeineldin and Kirtley 2009). This shortcoming of passive islanding is resolved by employing active islanding approaches, in which a disturbance is injected into the system following which the system's response is evaluated. Methods for active island detection include Sandia voltage shift, Sandia frequency shift, slip mode frequency shift and negative sequence current injection (Jang and Kim 2004; Liu et al. 2010; Lopes and Sun 2006; Trujillo et al. 2010; Karimi et al. 2008), and many others. Hybrid sensors are a combination of active and passive ways to overcome the shortcomings of the methods. Local approaches for island recognition utilise the communications infrastructure with DG as well as control centres. They have the benefit of no NDZ but the disadvantage of high costs.

The signal processing method is utilised so that the NDZ can be decreased while at the same time increasing the accuracy of the conventional approaches. Advanced signal processing techniques such as time-time transform, hybrid Stockwell transform, mathematical morphology, Hilbert Huang transform, Stockwell transform and wavelet Transform are utilised in this method for the purpose of discovering hidden data (Hsieh et al. 2008; Menezes et al. 2020; Mishra et al. 2017). These techniques are then applied to the signal processing. A classification learning algorithm is utilised by the intelligent islanding detection technique in order to identify islanding signals. Artificial neural network, decision tree, probabilistic neural network, support vector machine and fuzzy logic are the methods that are utilised the most frequently. This method has the challenge of determining an appropriate threshold, resulting in a significant increase in the amount of work that must be done (Raza et al. 2015).

In the field of distribution system protection, the spatiotemporal pattern-based detection approaches have become a current focus of discussion. These methods make use of aspects both temporal and spatial, including both of them simultaneously (Dubey et al. 2017; Sun et al. 2017). An online Bayes classifier that has been trained using spatiotemporal patterns is used to identify malicious cyber activity (Cui et al. 2020). In (Cui et al. 2019), the spatiotemporal correlation of µ-PMU data is utilised in an anomaly detection method that is suggested to use µ-PMU and a generalised graph Laplacian algorithm.

Reinforcement learning and extreme machine learning approaches are another area that has been discussed recently (Sahu et al. 2023). Reinforcement learning is used to a significant extent throughout the suggested energy storage system approach that is presented in (Oh and Hanho 2020). Chen et al. (2020) Presents a model-free control-based emergency plan that makes use of reinforcement learning and multi-q learning. In the paper referenced (Li et al. 2016), an extreme learning method is used.

In Liu et al. (2015), there is a proposal for island detection using PMU that is based on principal component analysis. An island index that is calculated using phase voltages that are measured using synchronised measurement technologies on both the side of the main grid and at the terminal of the generator is a technique that is presented in (Ostojic and Djuric 2018). Laverty et al. (2015) Makes use of a technique known as "continuous sync-check." Almas and Vanfretti (2015) presents an implementation of a hardware in loop island discovery algorithm that makes use of synchrophasor data. Some recent work on logic circuits and nano scale design is presented in (Ahmadpour et al. 2023a, b, c; Pramanik et al. 2023) that showcases the recent advancements in these areas.

The data transmission network that exists among measurement sites as well as PDCs is very important for the approaches that make use of PMUs or PMU data. Because of this, hackers have an opportunity to launch cyberattacks, which could result in incorrect classification. On the other hand, other approaches that don't use PMUs call for a distinct combination of software and hardware components, which drives up both the cost and the amount of time it takes to implement. Thus, in this paper, an intelligent strategy for island identification is proposed, in which the islanding detection is accomplished within the μ-PMU itself. The goal of this approach is to combine the benefits that are offered by both the PMU-based and the non-PMU-based methods. This will save time and money during implementation, and it will also protect the algorithm from being attacked via cyberspace.

1.3 Contributions

Listed below are the contributions of the suggested methodology for detection of islanding cases:

1. Traditional PMU based island detection implementations uses the information communication channel, whereas the proposed method does not. This will drastically lower the probability of a cyber-attack. Hence, this enhances the resilience of microgrid, particularly in terms of powering essential loads.
2. The approach detects island situations using the angular sum of the sequence negative phase angle and positive sequence phase angles.
3. The method is computationally efficient and possess a short response period of 15 ms. This short detection time will allow the DG to quickly regulate the power supply of the microgrid.

1.4 Paper organisation

The paper is separated into five units. Unit 2 presents an explanation of PMU and μ-PMU. In Unit 3, the proposed methodology is explained. The proposed procedure is verified under numerous circumstances and the consequences are provided in unit 4. Benefits of the technique is debated in the same unit. The complete method is summed up in unit 5.

2 PMU and μ-PMU

For a variety of purposes PMU has been used across the electrical system (Liu et al. 2020). A PMU makes an estimation of the phase angle as well as the magnitude of a synchronous current or voltage signal by means of a common time signal that is supplied by a GPS. The data congestion risk at the communication canal can be avoided using techniques such mentioned in Dubey et al. (2017). Nonetheless, the PMUs that are utilised in transmission systems are unable to be utilised in distribution systems due to the fact that distribution systems have a minimal phase angle variation between the buses that are closely situated. μ-PMUs were designed for distribution networks with the potential of having a resolution of microseconds with an accuracy of milli-degrees, which is one hundredth instances relative to the resolution of standard type PMU (Zhou et al. 2016). In addition to this, the harmonics and intermittent characteristics of the distribution system were taken into consideration during their design. These results can be obtained by using a high sampling rate in conjunction with a low total voltage deviation. A conventional μ-PMU has essentially the same design as the PMU. The power source is responsible for providing the μ-PMU with the necessary amount of electric power. All of the modules are linked to the electrical supply unit through their internal wiring. The three-phase voltage and current are provided by potential transformer (PT) and current transformer (CT), respectively, for the analog input. A device known as an anti-aliasing filter is applied to the input signal in order to remove frequencies that are higher than the Nyquist rate. After that, the signal is sent through an analog to digital converter (A/D) converter, and digital samples are taken as a result. A phase-locked oscillator and a GPS receiver are used to perform the sampling for the A/D converter. This ensures that the sampling is in sync with the clocked pulse cycle. In order to calculate magnitude and phase angle, discrete Fourier transform is implemented to all these digital samples as they are being processed by the CPU. After some particular instants, these time-stamped sequence components will be sent to the PDC via the communication channel (Murthy et al. 2014; Patnaik et al. 2020). Due to the fact that μ-PMU has a shorter connection length than PMU does, the level of cyber-attacks will be significantly lower. Hence, the μ-PMU is equipped with everything necessary to carry out detection of islands in the distribution side. In light of this fact, a new method for the passive detection of islanding using μ-PMUs is presented and described in this study.

In the suggested technique, the conventional construction of the μ-PMU (as described previously) is modified to some extent. In order to construct an island identification algorithm resistant to cyber-attack, the μ-PMU introduces a subsection that will only manage the island recognition process. Here, the filtered data are delivered straight to A/D converters, where sampling of data is performed without GPS. The data are then transmitted to a microprocessor for island detection, where they are analysed including an island detection algorithm. This part does not interfere with the normal operation of the μ-PMU. This component of the μ-PMU is implemented to lessen the likelihood of a GPS spoofing/jamming attack against the island finding algorithm. The subsection's method is designed such that it does not necessitate time-stamped phasors and therefore does not need the GPS signal. The usual μ-PMU procedure will be disrupted in the event of a GPS spoofing/jamming assault, but the island detecting mechanism will remain unaffected.

3 Methodology

The suggested technique is simulated for an IEEE 34 distribution network. A solar DG of 150 kW is added to one of the nodes. A μ-PMU is also added to the solar DG bus. The island scenarios are operated by opening the appropriate circuit breakers. In this method, the voltage signal of the solar generator is continuously analyzed by the μ-PMU. The μ-PMU then calculates the symmetrical components of the voltage. The angular sum of the positive and negative sequence components is evaluated with Fortescue transform in the μ-PMU. The graphs for several scenarios are simulated such as island, faults and normal conditions and are plotted in Figs. 2, 3, 4, 5, 6, 7. The graphs shows that the maximum value of angular sum is 90.72° for normal power system case, 181.2° for island case, 202.7° for line to line to line (LLL) fault case, 248.6° for line to line to ground (LLG) fault case, 174.2° for line to ground (LG) fault case and 93.21° for line to line (LL) fault case. Hence, the graphs show that the angular sum of the negative and positive sequence components is different for different scenarios.

3.1 Flow chart

Figure 8 depicts the proposed islanding detection method's flowchart. The suggested approach makes use of voltage measurements at predetermined DG locations over μ-PMU. In this case, the fixed frequency type sample clock is

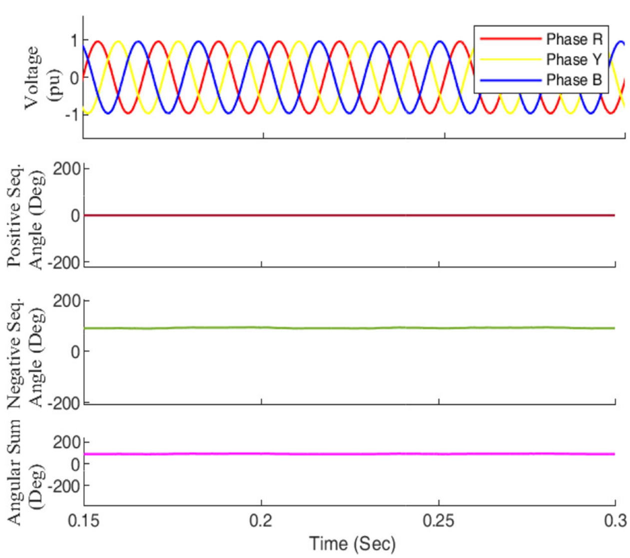

Fig. 2 Normal

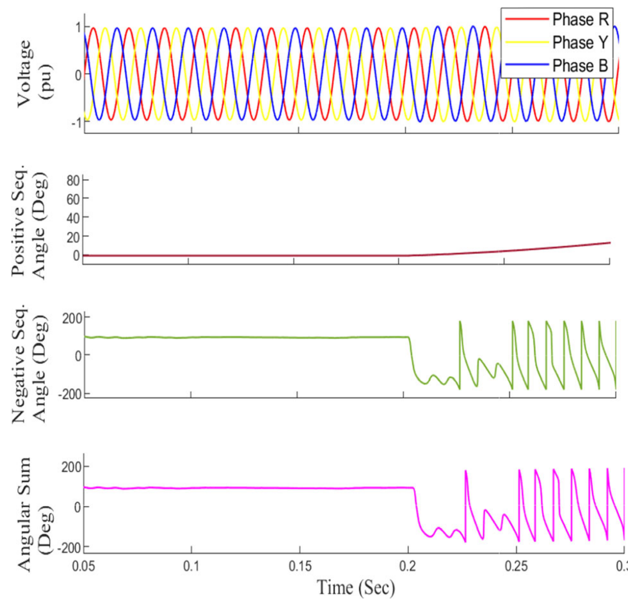

Fig. 3 Islanding

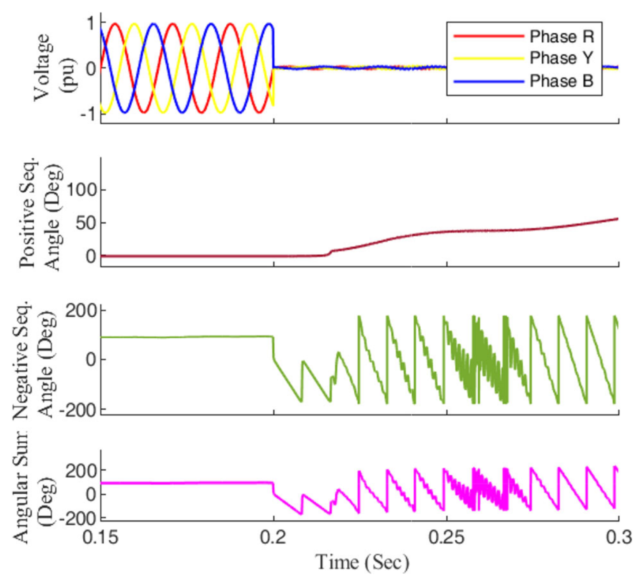

Fig. 4 Fault LLL

implemented and used for both nominal and off-nominal power system frequencies, with the sampling rate according to the given frequency. In most cases, a distortion is produced in the measurement during off-nominal frequencies of the power system, although this can be corrected with the use of appropriate filters. Nevertheless, the technique does not account for filtering this mistake at non-nominal frequencies. This is because locating islands as quickly as possible is a primary goal of the algorithm. The Fortescue transform then performs some additional processing on the detected voltage signal in order to determine the angular sum between the voltage positive sequence

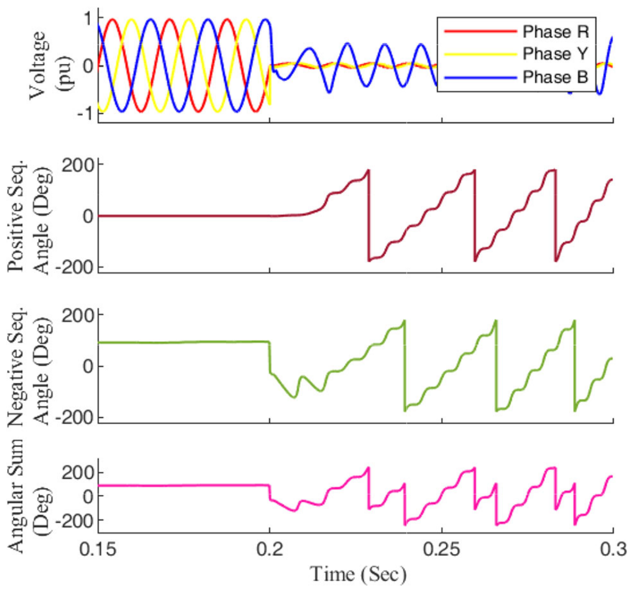

Fig. 5 LLG

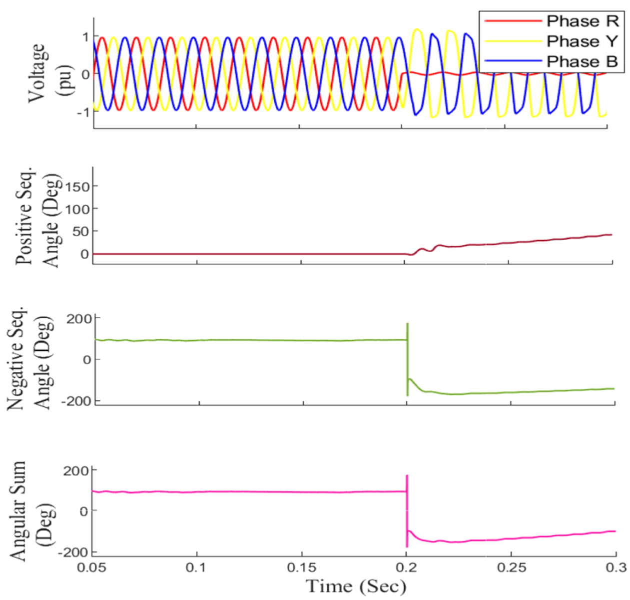

Fig. 6 LG

phase angle as well as the negative sequence phase angle. Following this step, the maximum value in voltage sequence phase angles will be calculated. If the calculated maximum value exceeds a threshold boundary, the procedure of isolating DG and the main grid will begin. After running a large number of simulations, the optimal value of the parameter is determined in order to achieve the ideal balance between the NDZ and the nuisance tripping of the relay. The explanations for the scenarios that can occur when trying to determine the threshold values can be found in Table 1. The time window frame is considered to be

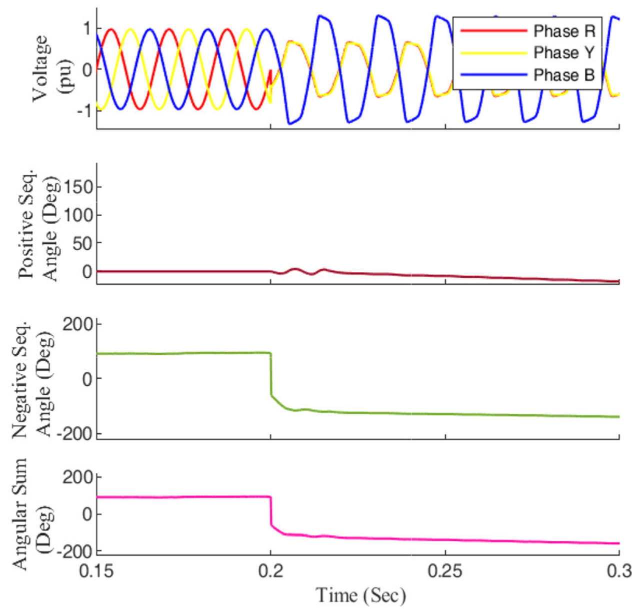

Fig. 7 LL

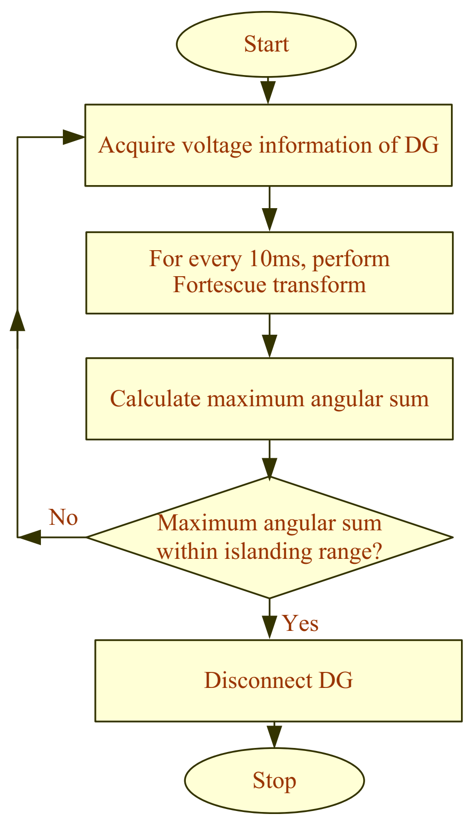

Fig. 8 Flow Chart

10 ms. The range of threshold values hence obtained is provided in Table 2.

Table 1 Situations inspected for threshold assessment

Situations	No. of situations	Description
Different faults	150	LG, LL, LLG, LLL faults
Islanding	150	Reactive and active power variation from 0 to 180 kVAR and 70–280 kW
Switching on of capacitor banks	120	60–180 kVAR in stages of 50
Switching on of loads	120	60–180 kW in stage of 50
Shedding of loads	120	60–180 kW in stage of 50

Table 2 Variation in values

Conditions	|Maximum sum| (Deg)
Islanding	180.3–184.7
Different faults	191.8–212.7 (LLL), 243.65–250.3 (LLG), 171.43–178.67 (LG), 92.9–94.7 (LL)
Normal/Other	90.8–92.3

4 Performance of the method

The suggested technique is evaluated via simulation for a variety of island, fault, and regular power energy system scenarios on the IEEE-34 node system. The criteria and outcomes are explained in the subsequent paragraphs.

To demonstrate that the complete network in the presented technique has no NDZ, an islanding scenario with zero reactive and active power imbalance between the local load and the DG is studied. The outcome is presented in Table 3. In addition to a power mismatch of zero, a number of different power mismatch situations (under island state) are considered, and the findings are summarized in the Table 3.

The faults LG, LLG, LL, and LLL at various sites (between node 836 and 862) are simulated, and the results of the simulation are reported in Table 4. Fault resistance (FR) is simulated to range from 0 to 100Ω, and the results of the simulation are given in Table 4. Fault inception angle (FIA) simulations were performed under the parameters described above, and the results of those simulations are reported in Table 4. The range of 0°–270° was chosen for the FIA simulations. It is possible to deduce from the table that the method employed works correctly in fault circumstances, meaning that it does not incorrectly categorise faults as being in an island circumstance.

Table 3 Performance at different power mismatch

Power mismatch (%)	|Maximum sum| (Deg)	Result of island detection
120	181.8	Positive
80	180.3	Positive
50	182.9	Positive
20	182.3	Positive
0	182.5	Positive
− 20	181.7	Positive
− 50	183.5	Positive
− 75	183.2	Positive
− 120	182.8	Positive

The algorithm is subjected to a number of additional tests, and the results of these tests are summarised in Table 5. This allows for a more thorough verification and examination of the method. Some examples of such situations comprise enlarging the islanded zone by activating the circuit breaker at node 834, moving the location of DG from node 838 to node 842, and then initiating islanding there. This outcome demonstrates that the process is effective in all cases and is not reliant on the islanded region, the arrangement of the system, or the position of the DG. In addition, the algorithm functions faultlessly in all other possible scenarios, such as the switching of a capacitor with a value of 125 kVAR at node-836 and the operation of an induction motor with a value of 75 kW at node-862.

The signals that are presented in Figs. 2, 3, 4, 5, 6, 7 are unpolluted and unaffected by any noise. Nonetheless, in real-world scenarios, there will invariably be some level of noise in the voltage signal as a result of the measurement, disturbance from neighbouring signals, and other factors. It’s possible that these disturbances will throw off the algorithm’s normal and smooth operation. So, the effect that noise has on an algorithm is a significant factor that plays a role in deciding the algorithm’s effectiveness. In order to do this, islanding scenarios with varying sound to noise ratio (SNR) have been taken into consideration for the suggested technique, and the results have been displayed in Table 6. From the table, it can be seen that the algorithm operates correctly in noisy surroundings with a

Table 4 Performance at different fault conditions

Conditions	|Maximum sum| (Deg)					Result of island detection
Fault type		LG	LL	LLG	LLL	
FR (Ω)	0	174.2	92.8	244.1	194.1	Negative
	25	172.3	92.6	245.8	192.2	Negative
	50	177.3	93.9	246.1	199.2	Negative
	75	178.1	92.9	245.9	201.9	Negative
	100	173.2	94.5	247.3	196.3	Negative
FIA (Deg °)	0	175.4	92.4	244.9	208.5	Negative
	30	176.3	92.5	243.0	199.8	Negative
	120	175.3	94.1	244.3	192.2	Negative
	240	171.9	93.5	248.1	197.3	Negative
	270	171.1	93.8	248.3	199.4	Negative

Table 5 Performance for different grid conditions

Conditions	|Maximum sum| (Deg)	Result of island detection
Islanding at 842 node number	181.87	Positive
Islanding at 834 node number	184.06	Positive
Induction Motor Starting	91.58	Negative
Capacitor Switching	92.17	Negative

signal-to-noise ratio of up to 35 dB. Nevertheless, the method generates incorrect results at levels higher than 35 dB. So, it is possible to draw the conclusion that the method described above is dependable and does not result in nuisance tripping even when subjected to a noise level constraint of 35 dB.

4.1 Assessment with other methods

Table 7 illustrates an assessment of the presented approach to other PMU or synchro phasor based island detection algorithms with regard to the consequences of various types of cyberattacks. Because each of the techniques relies on a communication channel and a GPS signal, it is simple to see that the vast majority of the algorithms are incapable of functioning properly in the face of a cyberattack. As a result, these approaches are more susceptible to cyber-attacks. The proposed technique, on the other hand, carries out detection of island inside the μ-PMU without making use of any reference phasor or any GPS signal, which means that the presented method has a lower risk of being subject to a cyber-assault. In spite of this, there is still a possibility of a cyber-breach occurring if the attacker attempts to directly penetrate the μ-PMU.

Table 6 Outcome for island conditions at different SNR

SNR (dB)	|Maximum sum| (Deg)	Result of island detection
10	182.75	Positive
15	183.11	Positive
25	181.96	Positive
35	183.16	Positive
45	182.87	Negative

To provide more evidence that the suggested approach is effective, it is contrasted with other approaches that operate under the same conditions as those presented in Table 8. All of the test scenarios is simulated in the programme MATLAB/SIMULINK R2022a, in the identical IEEE 34 network, on a computer equipped with an i7 CPU. This was done to ensure that the approaches are consistent with one another. In addition to the time it takes to execute the algorithm, the simulation of the procedures described in Murthy et al. (2014), Oh and Hanho (2020), Ostojić and Djurić (2018), Patnaik et al. (2020) takes into account a phasor calculation time delay of 5 ms with 40 ms communication latency. The table makes it clear that, with the exception of the final scenario, the suggested method performs better than the majority of the other methods when applied to different island scenarios. Because it has no communication delay and does not rely on any phasor calculations, the presented approach has a significantly faster island identification time compared to existing algorithms. This is because it eliminates the need for both of these factors. As a result, the method that has been proposed is significantly quicker.

Table 7 Comparison under different cyber-attacks

Scheme	Cyber Attack Type					
	Consequence of physically damaging the cables between PMUs and PDCs/Control Centres	Consequence of barricading the network traffics between PMUs and PDCs/Control Centres	Consequence of inoculation of false packets of PMU phasor data	Consequence of reiterating data	Consequence of Jam/spoof of GPS signal	Consequence of compromising of PMU
Principal component analysis (Liu et al. 2015)	May detect accurately (Rest on the VPN nature)	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately
Synchronized measuring technology (Ostojić et al. 2018)	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately
Loss of mains (Laverty et al. 2015)	Detect accurately (Uses traditional ROCOF or VS during this instant)	Detect accurately (Uses traditional ROCOF or VS during this instant)	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately
Real-time hardware-in-the-loop (Almas et al. 2015)	May detect accurately (Rests on the GOOSE message nature)	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately	Cannot detect accurately
Proposed	Detect accurately	Detect accurately	Detect accurately	Detect accurately	Detect accurately	Cannot detect accurately

GOOSE generic object-oriented substation events, *VPN* virtual private network, *VS* vector shift

Table 8 Comparison under various cases

Cases	Result of island detection				Detection time (ms)			
	Liu et al. (2015)	Ostojić et al. (2018)	Laverty et al. (2015)	Proposed	Liu et al. (2015)	Ostojić et al. (2018)	Laverty et al. (2015)	Proposed
15% power mismatch islanding	Positive	Positive	Positive	Positive	110	75	72	15
75% power mismatch islanding	Positive	Positive	Positive	Positive	108	55	67	15
Islanding under SNR 15 dB	Positive	Negative	Positive	Positive	111	–	62	15
Islanding under SNR 40 dB	Negative	Negative	Positive	Negative	–	–	65	–

5 Conclusion

Utilizing μ-PMU, this work proposes an improved and more intelligent method of islanding detection. The μPMU is configured to perform the sequence transform in order to determine the phase angle of the sequence components. The angular sum of the phase angles of a voltage signal's positive and negative sequences is utilized to detect island occurrence. The proposed algorithm is free of NDZ. To make the proposed approach resilient and reliable, it is simulated under multiple relevant scenarios, covering: islanding condition, normal condition, and LLL, LLG, LG, LL faults. Owing to the procedure being implemented within the μ-PMU, the probability of a cyberattack is minimized. Thus, results of the research show that such suggested technique of islanding detection is not only fast, but is also easier, economical, secure, more precise, and quick on the uptake.

There are numerous opportunities to consider for future research. Bearing in mind the ultra-fast charging techniques of electric automobiles that might generate grid transients equivalent to signals of island detection, the current approach may be expanded to grids with a significant electric automobiles' penetration. Since the current approach has limitations, modern improved methods like optimization algorithms, spatiotemporal pattern and extreme learning may be integrated to address its flaws. With the increasing complexity of the electrical infrastructure and the scope of cyber risks, these technologies might also prove useful. In addition, future study can consider management of power flow strategies within the islanded area by segregating it in multiple smaller islands and may be called as island of islands. Further, any real-world implementations where this smart island detection application may be applied successfully can also be regarded as an extension of this work so that the outcomes and benefits may be observed in those scenarios in real time.

Author contributions All authors contributed to the study, conception and design. Material preparation, data collection and analysis were performed by AS. The first draft of the manuscript was written by AS and SD. All authors read and approved the final manuscript.

Funding Open access funding provided by Manipal Academy of Higher Education, Manipal. The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data availability All data included in this paper are available upon request by contact with the corresponding author.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

Abd-Elkader AG, Saleh SM, Eiteba MM (2018) A passive islanding detection strategy for multi-distributed generations. Int J Electr Power Energy Syst 99:146–155

Admasie S, Bukhari SBA, Haider R, Gush T, Kim CH (2019) A passive islanding detection scheme using variational mode decomposition-based mode singular entropy for integrated microgrids. Electr Power Syst Res 177:105983

Ahmad KNEK, Selvaraj J, Abd Rahim N (2013) A review of the islanding detection methods in grid-connected PV inverters. Renew Sustain Energy Rev 21:756–766

Ahmad T, Madonski R, Zhang D, Huang C, Mujeeb A (2022) Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: key developments, challenges, and future research opportunities in the context of smart grid paradigm. Renew Sustain Energy Rev 160:112128

Ahmadpour SS, Navimipour NJ, Mosleh M, Bahar AN, Yalcin S (2023a) A nano-scale n-bit ripple carry adder using an optimized XOR gate and quantum-dots technology with diminished cells and power dissipation. Nano Commun Networks 36:100442

Ahmadpour SS, Heidari A, Navimpour NJ, Asadi MA, Yalcin S (2023b) An efficient design of multiplier for using in nano-scale IoT systems using atomic silicon. IEEE Internet of Things J 10:14908–14909

Ahmadpour SS, Navimipour NJ, Bahar AN, Mosleh M, Yalcin S (2023c) An energy-aware nano-scale design of reversible atomic silicon based on Miller algorithm. IEEE Des Test 40:62–69

Almas MS, Vanfretti L (2015) RT-HIL implementation of the hybrid synchrophasor and GOOSE-based passive islanding schemes. IEEE Trans Power Deliv 31(3):1299–1309

Ashour M, Ben-Brahim L, Gastli A, Al-Emadi N, Fayyad Y (2013) Matlab/Simulink implementation & simulation of islanding detection using passive methods. In: 2013 7th IEEE GCC conference and exhibition (GCC). IEEE, pp. 320–325

Bahrani B, Karimi H, Iravani R (2009) Nondetection zone assessment of an active islanding detection method and its experimental evaluation. IEEE Trans Power Deliv 26(2):517–525

Chen C, Cui M, Li F, Yin S, Wang X (2020) Model-free emergency frequency control based on reinforcement learning. IEEE Trans Ind Inform 17:2336–2346 (**in press**)

Cui M, Wang J, Florita AR, Zhang Y (2019) Generalized graph Laplacian based anomaly detection for spatiotemporal micro-PMU data. IEEE Trans Power Syst 34(5):3960–3963

Cui M, Wang J, Chen B (2020) Flexible machine learning-based cyberattack detection using spatiotemporal patterns for distribution systems. IEEE Trans Smart Grid 11(2):1805–1808

De S, Sodhi R (2022) A PMU assisted cyber attack resilient framework against power systems structural vulnerabilities. Electr Power Syst Res 206:107805

Dey B, Dutta S, Garcia Marquez FP (2023) Intelligent demand side management for exhaustive techno-economic analysis of micro-grid system. Sustainability 15(3):1795

Dubey R, Samantaray SR, Panigrahi BK (2017) An spatiotemporal information system based wide-area protection fault identification scheme. Int J Electr Power Energy Syst 89:136–145

Duo W, Zhou MengChu, Abusorrah A (2022) A survey of cyber attacks on cyber physical systems: recent advances and challenges. IEEE/CAA J Autom Sin 9(5):784–800

Dutta S, Sadhu PK, Reddy MJB, Mohanta DK (2020) Role of microphasor measurement unit for decision making based on enhanced situational awareness of a modern distribution system. Decision making applications in modern power systems. Academic Press, pp 181–199

Dutta S, Sadhu PK, Cherikuri M, Mohanta DK (2022a) Application of artificial intelligence and machine learning techniques in island detection in a smart grid. Intelligent renewable energy systems. Wiley, pp 79–109

Dutta S, Sahu SK, Dutta S, Dey B (2022b) Leveraging a micro synchrophasor for fault detection in a renewable based smart grid—a machine learned sustainable solution with cyber-attack resiliency. E-Prime-Adv Electr Eng Electron Energy 2:100090

Dutta S, Sahu SK, Roy M, Dutta S (2023) A data driven fault detection approach with an ensemble classifier based smart meter in modern distribution system. Sustain Energy Grids Netw 34:101012

Freitas W, Xu W, Affonso CM, Huang Z (2005) Comparative analysis between ROCOF and vector surge relays for distributed generation applications. IEEE Trans Power Deliv 20(2):1315–1324

Gupta P, Bhatia RS, Jain DK (2016) Active ROCOF relay for islanding detection. IEEE Trans Power Deliv 32(1):420–429

Hsieh CT, Lin JM, Huang SJ (2008) Enhancement of islanding-detection of distributed generation systems via wavelet transform-based approaches. Int J Electr Power Energy Syst 30(10):575–580

Jang SI, Kim KH (2004) An islanding detection method for distributed generations using voltage unbalance and total harmonic distortion of current. IEEE Trans Power Deliv 19(2):745–752

Karimi H, Yazdani A, Iravani R (2008) Negative-sequence current injection for fast islanding detection of a distributed resource unit. IEEE Trans Power Electron 23(1):298–307

Larik NA, Tahir MF, Elbarbary ZS, Yousaf MZ, Khan MA (2022) A comprehensive literature review of conventional and modern islanding detection methods. Energ Strat Rev 44:101007

Laverty DM, Best RJ, Morrow DJ (2015) Loss-of-mains protection system by application of phasor measurement unit technology with experimentally assessed threshold settings. IET Gener Transm Distrib 9(2):146–153

Li Z, Ye L, Zhao Y, Song X, Teng J, Jin J (2016) Short-term wind power prediction based on extreme learning machine with error correction. Protect Control Modern Power Syst 1(1):1–8

Liu F, Kang Y, Zhang Y, Duan S, Lin X (2010) Improved SMS islanding detection method for grid-connected converters. IET Renew Power Gener 4(1):36–42

Liu X, Laverty DM, Best RJ, Li K, Morrow DJ, McLoone S (2015) Principal component analysis of wide-area phasor measurements for islanding detection—a geometric view. IEEE Trans Power Deliv 30(2):976–985

Liu S, Zhuang S, Xu Q, Xiao J (2016) Improved voltage shift islanding detection method for multi-inverter grid-connected photovoltaic systems. IET Gener Transm Distrib 10(13):3163–3169

Liu Y, Wu L, Li J (2020) D-PMU based applications for emerging active distribution systems: a review. Electr Power Syst Res 179:106063

Lopes LA, Sun H (2006) Performance assessment of active frequency drifting islanding detection methods. IEEE Trans Energy Convers 21(1):171–180

Menezes TS, Fernandes RA, Coury DV (2020) Intelligent islanding detection with grid topology adaptation and minimum non-detection zone. Electr Power Syst Res 187:106470

Mirshekali H, Dashti R, Keshavarz A, Shaker HR (2022) Machine learning-based fault location for smart distribution networks equipped with micro-PMU. Sensors 22(3):945

Mishra M, Sahani M, Rout PK (2017) An islanding detection algorithm for distributed generation based on Hilbert–Huang transform and extreme learning machine. Sustain Energy, Grids Netw 9:13–26

Mishra M, Chandak S, Rout PK (2019) Taxonomy of islanding detection techniques for distributed generation in microgrid. Renew Energy Focus 31:9–30

Murthy C, Mishra A, Ghosh D, Roy DS, Mohanta DK (2014) Reliability analysis of phasor measurement unit using hidden Markov model. IEEE Syst J 8(4):1293–1301

Oh E, Hanho W (2020) Reinforcement-learning-based energy storage system operation strategies to manage wind power forecast uncertainty. IEEE Access 8:20965–20976

Ostojić MM, Djurić MB (2018) The algorithm with synchronized voltage inputs for islanding detection of synchronous generators. Int J Electr Power Energy Syst 103:431–439

Patnaik B, Mishra M, Bansal RC, Jena RK (2020) AC microgrid protection—a review: current and future prospective. Appl Energy 271:115210

Pramanik AK, Mahalat MH, Pal J, Ahmadpour SS, Sen B (2023) Cost-effective synthesis of QCA logic circuit using genetic algorithm. J Supercomput 79(4):3850–3877

Raza S, Mokhlis H, Arof H, Laghari JA, Wang L (2015) Application of signal processing techniques for islanding detection of distributed generation in distribution network: a review. Energy Convers Manag 96:613–624

Redfern MA, Usta O, Fielding G (1993) Protection against loss of utility grid supply for a dispersed storage and generation unit. IEEE Trans Power Deliv 8(3):948–954

Sahu SK, Roy M, Dutta S, Ghosh D, Mohanta DK (2023) Machine learning based adaptive fault diagnosis considering hosting capacity amendment in active distribution network. Electr Power Syst Res 216:109025

Shukla A, Sadhu PK, Dutta S, Sahu SK, Dey B (2023a) An island detection approach in 6G paradigm for an active distribution network—a future perspective for next generation smart grids. Comput Electr Eng 111:108932

Shukla A, Dutta S, Sahu SK, Sadhu PK (2023b) A narrative perspective of island detection methods under the lens of cyber-attack in data-driven smart grid. J Electr Syst Inform Technol 10(1):1–32

Sun S, Yang Q, Yan W (2017) Optimal temporal-spatial PEV charging scheduling in active power distribution networks. Protect Control Modern Power Syst 2(4):379–388

Trujillo CL, Velasco D, Figueres E, Garcerá G (2010) Analysis of active islanding detection methods for grid-connected microinverters for renewable energy processing. Appl Energy 87(11):3591–3605

Xie X, Huang C, Li D (2020) A new passive islanding detection approach considering the dynamic behavior of load in microgrid. Int J Electr Power Energy Syst 117:105619

Zeineldin HH, Kirtley JL Jr (2009) Performance of the OVP/UVP and OFP/UFP method with voltage and frequency dependent loads. IEEE Trans Power Deliv 24(2):772–778

Zhou Y, Arghandeh R, Konstantakopoulos I, Abdullah S, von Meier A, Spanos CJ (2016) Abnormal event detection with high resolution micro-PMU data. In: 2016 Power Systems Computation Conference (PSCC). IEEE, pp. 1–7