A State Partition Particle Filter based Approach for Detection of Switching Attack

Yadav, Seema ; Kishor, Nand ; Purwar, Shubhi ; Subramaniam Rajkumar, Vetrivel; Stefanov, Alexandru

DOI
10.1109/SmartGridComm60555.2024.10738041

Publication date
2024

Document Version
Final published version

Published in
Proceedings of the 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)

2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) | 979-8-3503-1855-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/SmartGridComm60555.2024.10738041

A State Partition Particle Filter based Approach for Detection of Switching Attack

Seema Yadav
Department of Electrical Engineering
Motilal Nehru National Institute of Technology
Prayagraj, India
seemayadaven1041@gmail.com

Nand Kishor
Department of Engineering
Østfold University College
Fredrikstad, Norway
nand.kishor@hiof.no

Shubhi Purwar
Department of Electrical Engineering
Motilal Nehru National Institute of Technology
Prayagraj, India
shubhi@mnnit.ac.in

Vetrivel Subramaniam Rajkumar
Department of Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
v.subramaniamrajkumar@tudelft.nl

Alexandru Ștefanov
Department of Electrical Sustainable Energy
Delft University of Technology
Delft, The Netherlands
A.I.Stefanov@tudelft.nl

Abstract— **The increasing risk of cyber-physical attacks (CPAs) on power infrastructure has led to need for reliable detection technologies. As the landscape of cyber threats evolves, it becomes imperative to continually update and enhance attack detection techniques. This research investigates the formulation of detection algorithm, via combination of State Partition Particle Filter (SP-PF) theories for power system security. The proposed approach applies intelligent partitioning of the state space so as to be accurately represented with fewer particles. This reduction in computational demand enhances the algorithm's efficiency, making it more practical for real-time applications. The detection algorithm based on SP-PF is tested against switching attacks (SAs) launched on the governor and excitation systems associated with the generator. The RTDS platform is utilized for conducting real-time simulations of IEEE 9-bus power network in order to demonstrate the efficacy of proposed SP-PF based detection SA in real-time.**

Keywords—cyber-physical attack detection, state-partition, particle-filter, estimation, real-time simulation, switching attack.

I. INTRODUCTION

Security forms the bedrock of any system's resilience and future sustainability. In acknowledging this fundamental aspect, the imperative of upgrading security measures cannot be overstated. While predicting the probability of cyber-physical attacks (CPAs) remains elusive, recent events, notably the Ukraine nuclear power plant case, underscore the critical need to fortify our power systems. Just as computer systems undergo routine upgrades, so too must power plants evolve, prioritizing robust security protocols.

As a reaction to the increasing menace of cyber-attacks, a variety of techniques for detecting such attacks have surfaced, generally classified into two frameworks: Reference model-based detection (RMD) and Machine Learning-based detection (MLD) [1]. RMD methodologies apply changes in system states, whereas MLD methods involve the training of classifiers for attack identification.

RMD involves two stages: estimating the system's internal states and processing both measured and estimated data, with discrepancies assessed through similarity tests [2]. State estimation is classified into static and dynamic types [3]. Static state estimation [4] determines the power system's state at a specific moment, using data from phasor measurement units (PMUs) and SCADA systems. Techniques include weighted least squares [5] for minimizing differences, the Gauss-Newton method [6] for linear approximations, maximum likelihood estimation [7] for maximizing observed measurement probabilities, kalman filtering [8] for dynamic systems with noise, and sparse estimation [9] to reduce computational complexity. However, the techniques mentioned above fail to account for changes caused by fluctuations in load, generation, or CPAs, which are critical for real-time monitoring and control. Deep learning methods like recurrent neural network (RNN), fully-connected neural network (FCN), and convolutional neural network (CNN) detect CPAs but may overlook system properties [10]. In [11], estimation offers robust FDI detection, yet it's limited by reliance on datasets. This exposes vulnerabilities to adversarial attacks, highlighting the need for improved defense strategies.

Dynamic state estimation assumes a pivotal role in real-time power system management. It empowers operators to navigate dynamic events, ensuring grid stability, reliability, and efficiency amid contingencies, load variations, and faults, through continuous and precise system-state insights. Various dynamic state estimation techniques cater to different system nuances. The extended kalman filter extends the conventional kalman filter for nonlinear systems, often applied in estimating nonlinear power system states [12]. The unscented kalman filter [13], ideal for highly nonlinear systems, selects representative sample points deterministically. Particle filters [14], beneficial in non-gaussian and highly nonlinear systems, estimates system states using a particle ensemble. Sequential monte-carlo methods or particle filters leverage random samples to converge on true system states iteratively. Machine learning-based attack detection in power systems involves the utilization of advanced algorithms and predictive analytics to identify anomalous patterns, recognize potential threats, and fortify the resilience of the infrastructure [15].

Detection tests for CPAs in power systems, assessing disparities through various similarity tests is a crucial aspect. Particle filtering is recognized as a significant similarity test, but its adaptability to sudden changes in system dynamics, especially those induced by CPAs, can be limited. Notably, state partition particle filters emerge as a promising solution,

introducing a more structured approach to navigate shifts in the state space. This structured approach enhances adaptability in scenarios marked by abrupt changes. Furthermore, the challenge of accurately tracking multimodal distributions, where the system state can exist in multiple distinct modes, poses a difficulty for traditional particle filters. State partition particle filters, with their emphasis on specific partitions of the state space, offer a potential solution by providing a more nuanced and targeted approach to capture and track multimodal distributions effectively. This nuanced approach demonstrates the potential of state partition particle filters in addressing the limitations associated with traditional particle filters, contributing to the advancement of reliable detection mechanisms in the context of power system cybersecurity [16]-[17].

The contributions of this research paper can be summarized as follows:

1. This study extends the already reported SAs [18], which has shed light on the vulnerabilities of power systems to SAs and thus contribute valuable insights into the development of robust detection mechanisms in context of power system security. The detection of SAs has not been thoroughly explored in existing literature.
2. One primary contribution of this research lies in the introduction and exploration of State-Partition Particle Filter (SP-PF) as a novel approach for SAs detection in power systems. While particle filter-based attack detection methods are well-established, the application of SP-PF specifically for this purpose has not been thoroughly studied in existing literature. This research pioneers the utilization of SP-PF as a technique to enhance the robustness and accuracy of CA detection in power systems.
3. This study developes strong mathematical formulation via augmentation of individual techniques; SP and PF towards attack detection. The paper delves into the theoretical foundations of SP-PF, providing a comprehensive examination of its mathematical underpinnings in the context of CPAs in power systems. This analysis is critical for establishing a sound theoretical framework and understanding the intricacies of SP-PF-based CA detection.

By delineating these contributions, this research paper aims to not only advance the current state of knowledge in the field of power system security but also to stimulate further research endeavors in the promising domain of SP-PF based CA detection. The remaining sections of the manuscript are as follows. Section II presents the power network model used in this study, followed by Section III discussing formulation of SP-PF theories for CA detection. Section IV presents the discussion on real-time set-up developed for performing study. Section V discusses the results on CA detection and finally conclusions are drawn in Section VI.

II. Power Network Model And Its Description

The IEEE 9-bus power system network [19] as shown in Fig. 1 is used as a test canvas. The representation of power components, including circuit breakers (CBs) are exactly the same as referred in [18]. The use of same network parameters and operating conditions allow for a deeper understanding of system dynamics on account of CA, aiding in the development of more robust and efficient detection algorithm. The system parameters as a reference are given in Table I in Appendix section. Each generator in the network is represented by the following 4th-order differential equations given as [20]:

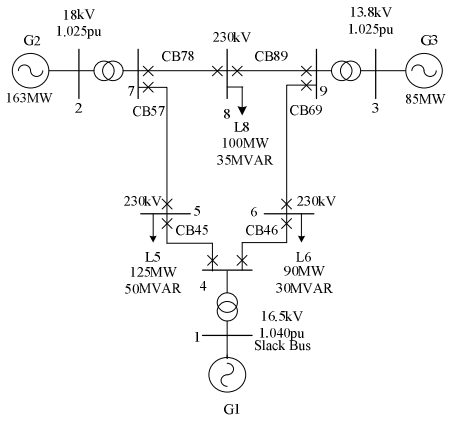

Fig. 1. IEEE 9-bus power network

$$\dot{\delta} = \omega_0 \Delta\omega \tag{1}$$

$$\Delta\dot{\omega} = \frac{1}{2H}(T_m - T_e - K_D\Delta\omega) \tag{2}$$

$$\dot{e}'_q = \frac{1}{T'_{do}}(E_{fd} - e'_q - (x_d - x'_d)i_d) \tag{3}$$

$$\dot{e}'_d = \frac{1}{T'_{qo}}(-e'_d - (x_q - x'_q)i_q \tag{4}$$

In the given context, δ represents the rotor angle in radians, $\Delta\omega$ signifies the rotor speed deviation, e'_d and e'_q denote the transient voltages along the d and q axes, respectively. T_m stands for the mechanical torque, T_e represents the electric air-gap torque, E_{fd} is the internal field voltage, ω_0 is the nominal value of angular frequency, H is the inertia constant, and K_D is the load damping constant. Additionally, T'_{do} and T'_{qo} represent the open-circuit time constants in the direction of the d and q axes, while x_d and x_q are the synchronous reactance at the d and q axes, respectively. Lastly, x'_d and x'_q denote the transient reactance along the d and q axes.

Each generator is associated with its excitation system and governor, and operated such as to maintain integrity of the entire power network. The control parameters of these are referred from [18].

III. Detection Algorithm

This section presents the basics of particle filter, and state partition particle filter and its formulation for CA detection problem.

A. Particle Filter (PF)

The PF is a technique used in probabilistic estimation, particularly in scenarios involving nonlinear and non-Gaussian systems. Its fundamental concept revolves around representing the posterior probability density function using a collection of random samples or particles, each associated with a weight. Instead of directly calculating the posterior density function, which can be complex or intractable in many real-world scenarios, the PF approximates this density function using these particles and their weights. These

particles are drawn from a proposed distribution, often referred to as the importance density or proposal distribution. The weights assigned to these particles reflect their relative likelihood or importance in representing the true underlying distribution of the system states.

To facilitate the PF application, the state equations representing the generator dynamics (1-4), including those of excitation and governor system can be re-written in a general state space form as in (5-11):

$$\dot{x} = f_c(x,u) + w_c \tag{5}$$

$$y = h_c(x,u) + v_c \tag{6}$$

$$E[w_c w_c^T] = Q \tag{7}$$

$$E[v_c v_c^T] = R \tag{8}$$

$$x = \left[\delta\ \Delta\omega\ e_q'\ e_d'\right]^T \tag{9}$$

$$u = \left[T_m\ E_{fd}\ i_R\ i_I\right]^T \tag{10}$$

$$y = [e_R\ e_I]^T \tag{11}$$

In this context, x denotes the state vector, u represents the input vector, and y is the output vector. The functions $f_c(*)$ and $h_c(*)$ correspond to the state transition and output functions, respectively. The subscript 'c' signifies the continuous form of the equations. The vectors w_c and v_c stand for the process and output noise, respectively, modeled as white noise with covariance matrices defined by (7) and (8).

To apply a Particle Filter (PF) on discrete measurements, it is necessary to discretize the continuous equations (5-11) into a discrete model as outlined in (12-13), where the subscript indicates the time at $k\Delta t$.

$$x_k = f(x_{k-1}, u_{k-1}) + w_{k-1} \tag{12}$$

$$y_k = h(x_k, u_k) + v_k \tag{13}$$

The Euler method [21] is utilized to discretize the general state-space (5), which represents the state equations of the power system network, in each time step as described in (14). Here, $\tilde{f}_c$ can be computed using equations (15) and (16). Additionally, w_{k-1} denotes the discrete process noise.

$$x_k \approx x_{k-1} + \tilde{f}_c \Delta t + w_{k-1} \tag{14}$$

$$\tilde{f}_c = (f_c(\tilde{x}_k, u_k) + f_c(x_{k-1}, u_k))/2 \tag{15}$$

$$\tilde{x}_k = x_{k-1} + \Delta t \cdot f_c(x_{k-1}, u_{k-1}) \tag{16}$$

$$Q_d \triangleq E(w_{k-1} w_{k-1}^T) \tag{17}$$

Output function (6) can be discretized as (18), with the discrete output noise

$$y_k = h_c(x_k, u_k) + v_k \tag{18}$$

$$R_d \triangleq E(v_k v_k^T) \tag{19}$$

B. State Partition Particle Filter (SP-PF)

SP-PF is a specialized variant of particle filter designed to handle high-dimensional state spaces more efficiently. It divides the state space into smaller, more manageable partitions. This division reduces the curse of dimensionality, making it easier to represent and track the state space accurately with a smaller number of particles. Additionally, partitioning the state space allows, for more focused sampling within each partition. Instead of spreading particles uniformly across the entire space, particles are concentrated in regions that are more likely to contain the true state, improving accuracy.

The SP-PF partitions the state at time t as $x_t = [x_{1,t}^T, x_{2,t}^T, \ldots, x_{k,t}^T]$, where $x_{k,t} \epsilon \mathbb{R}^{d_x}$ is the state vector of partition k. Each partition is handled by a distinct PF, and there is no requirement for all partitions to have the same size. The kth PF approximates the marginal posterior $p(x_{k,t}|y_t)$ by generating a discrete random measure $\chi_{k,t} = \{x_{k,t}^{m_k}, w_{k,t}^{m_k}\}_{m_k=1}^{M_k}$, consisting of M_k particles $x_{k,t}$ and their corresponding weights $w_{k,t}$. The workflow of SP-PF for a specific time instant t can be succinctly summarized through the following steps:

4. At time t, each filter k proposes M_k particles by sampling

$$x_{k,t}^{mk} \sim p\left(x_{k,t} \middle| x_{k,t-1}^{mk}, \hat{x}_{-k,t-1}\right) \tag{20}$$

where $m_k = 1, \ldots, M_k$. Here, $\hat{x}_{-k,t-1}$ represents the estimates of all partitions from the previous time step except the kth, i.e., $\hat{x}_{-k,t-1}^{\top} = [\hat{x}_{1,t-1}, \ldots, \hat{x}_{k-1,t-1}, \hat{x}_{k+1,t-1}, \ldots, \hat{x}_{K,t-1}]$.

These estimates are obtained through the exchange of information from the other filters at the end of the previous time step.

5. The proposed particles can be used to obtain predictions of the current state x_t as:

$$\tilde{x}_{k,t} = \frac{1}{M_k} x_{k,t}^{(mk)} \tag{21}$$

The kth filter transmits these predictions to the remaining filters and receives predictions, denoted as $\tilde{x}_{-k,t}$, from the other filters. Here, $\tilde{x}_{-k,t}$ is defined similarly to $\hat{x}_{-k,t-1}$.

6. The filters use the obtained predictions and estimates to update the weights in accordance with $\tilde{w}_{k,t}^{(mk)} \propto \tilde{w}_{k,t-1}^{(mk)} \frac{p\left(y_t \middle| x_{k,t}^{(mk)}, \tilde{x}_{-k,t}\right) p\left(x_{k,t}^{mk} \middle| \hat{x}_{-k,t-1}\right)}{q\left(x_{k,t}^{(mk)} \middle| \hat{x}_{-k,t-1}, y_t\right)}$ (22)

In this context, the top part of the fraction signifies the probability and transition density, while the bottom part corresponds to the assessment of the proposal distribution at the m_kth particle (refer to [22], [23] for detailed definitions and derivations of PF). The adjustment factor is an approximation since it relies on predictions and estimates of all state partitions except the kth element.

7. Normalize above estimated weights as

$$w_{k,t}^{mk} = \frac{\tilde{w}^{(mk)k,t}}{\sum_{n=1}^{M_k} \tilde{w}_{k,t}^{(n)}},\ m_k = 1, \ldots, M_k \tag{23}$$

8. Obtain the state estimates for each partition $x_{k,t}$ using the weights, for e.g.

$$\hat{x}_{k,t} = \sum_{m_k=1}^{M_k} w_{k,t}^{(mk)} \, x_{k,t}^{mk} \quad (24)$$

9. Implement iterative resampling if needed to prevent weight degeneracy [23].

10. Identify the occurrence of the SA using the procedures outlined in the section III (C).

C. SP-PF based Detection

In this subsection, we explore the approach to identifying CA, specifically SA, using the information derived from the SP-PF. Beyond the challenge of filtering a signal, there exists the task of determining the presence or absence of SA. This is commonly referred to as the detection problem [24]. Considering two hypotheses:

•$\mathcal{H}_0$: CPS absent

$$x(k) = f(x_{k-1}, u_{k-1}) + w_{k-1}$$

• $\mathcal{H}_1$: CPS present

$$x(k) = g\{f(x_{k-1}, u_{k-1}) + w_{k-1}\}$$

where, x_{k-1} evolves according to system (12-13)

The likelihood ratio is defined by:

$$L(X_k) = \frac{p(x_1, \dots, x_k|\mathcal{H}_1)}{p(x_1, \dots, x_k|\mathcal{H}_0)} \quad (25)$$

The SA is declared to be present whenever, the likelihood $L(X_k)$ exceeds a threshold τ (a user defined threshold value) thus, when

$$L(X_k) > \tau \quad (26)$$

In study the value of threshold τ is calculated for study system following discussions given in [22].

The likelihood ratio test is employed to detect SA. The likelihood ratio will vary according to state variable under normal and SA conditions.

IV. Real-Time Setup

Fig. 2 illustrates the application of a SA logic implemented on power components; excitation system (ES) and governor system (GS) as explored in [25]. The construction of a successful SA involves the use of an intruder device that establishes a stable sliding surface and operates at a unique switching instant obtained from the phase portrait. The phase portrait serves as a graphical representation of two crucial state variables of the system, namely the rotor angle and rotor speed of the generator. The SA indirectly manipulates the switches corresponding to the excitation system and governor system, rendering them operative and idle between two specific time instants. During the periods, when the switch is operative and idle, the system exhibits two distinct characteristics, thereby referred to as Subsystem A_1 and Subsystem A_2. The SA operates the switch between these subsystems continuously until the power system becomes inherently unstable. This deliberate manipulation and oscillation between subsystems to contribute towards destabilization of the overall system, emphasizing the potency of SAs in compromising power system stability. The utilization of the phase portrait and the dynamic switching mechanism adds a layer of complexity to the attack strategy, making it essential to employ advanced detection and mitigation techniques, such as the proposed SP-PF to safeguard the power system against such threats.

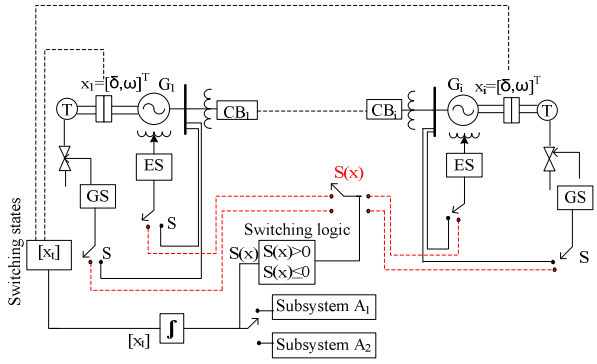

Fig. 2. Illustration of SA on power components [17]

In study, a real-time simulation setup, i.e. real-time digital simulator (RTDS) is developed to monitor and demonstrate the ability of proposed SP-PF for detection of SA in real-time. The schematic is shown in Fig. 3. The said setup consists of three interconnected systems; the first one incorporates the SP-PF algorithm implemented in MATLAB, while the second system features a 9-bus power network model simulated in RSCAD and third one consists of SA logic being accessed by intruder. The integration of these three systems is achieved through the use of the TCP/IP protocol, enabling seamless communication between the developed detection algorithm and the power network. Within this framework, the primary focus is on the continuous estimation of the power system's states, with specific emphasis on the rotor angle state variable, utilizing the SP-PF algorithm. The rotor angle is a significant state variable indicating the power system stability. To simulate realistic scenarios and assess the resilience of the system, the SA is introduced on ES and GS. This intentional switching of control parameters induces instability within the system as discussed in [25].

As discussed in next section, the SP-PF algorithm calculates a likelihood ratio that dynamically evolves over time. This evolving likelihood ratio is then compared against predefined threshold value. The continuous monitoring of the likelihood ratio allows for the timely detection of deviations from the normal behavior, indicating the presence of SA in the power network. With implementation of detection algorithm in real time, the research aims to enhance the understanding of power system stability under dynamic conditions and provide valuable insights into the effectiveness of the SP-PF algorithm in detection of SA.

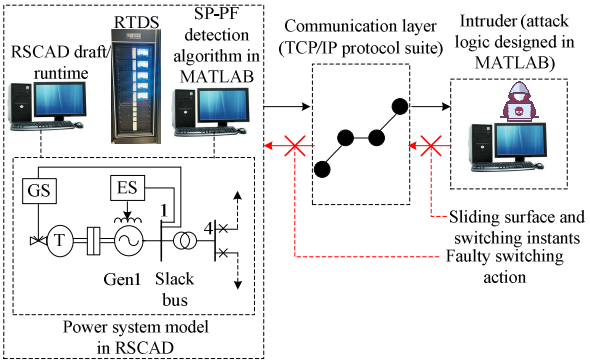

Fig. 3. Real-time simulation setup for SA detection

V. Real-Time Simulation Results

The primary focus of this study is to detect implementation of SA introduced on ES and GS, associated with the generator in the power network. As discussed later in the section, the real-time simulation results reveal the effectiveness of the proposed detection algorithm in promptly identifying the SA. The SP-PF exhibits a high degree of accuracy in distinguishing between normal system behavior and malicious switching events, showcasing its potential as a reliable detection mechanism.

A. Detection of SA introduced in ES

As an illustration, the SA is applied on the ES of generator G1 for different operating conditions; changes in active power/reactive power. The SA is launched at 1 sec and remains applicable until 5sec. In Fig. 4(a), variation in likelihood ratio is depicted under base power operating conditions of power network. The likelihood ratio, being state-dependent, exhibits dynamic changes over time following the initiation of the attack. Detection of the attack occurs when this likelihood ratio surpasses the predefined threshold limit, which is calculated as -3.72×10^{-5} [24]. Similarly, in Figs. 4(b)-4(d), the results on variation in likelihood ratio is shown for 50% change in active power, 50% change in reactive power and 30% change in reactive power respectively from base load condition.

The outcomes demonstrate the successful detection of the SA using the SP-PF technique under these altered operating conditions. The algorithm proves its efficacy in identifying deviations caused by the SA from normal the behavior, thus reinforcing its utility as a reliable tool for detecting and mitigating SAs in power network. The ability to detect variations in active and reactive power highlights the algorithm's sensitivity to changes in the system dynamics, emphasizing its potential for enhancing the security and resilience of power systems against malicious attacks.

Further, it should be noted that after elapse of SA at 5 sec, the likelihood ratio follows its trend below the threshold scale.

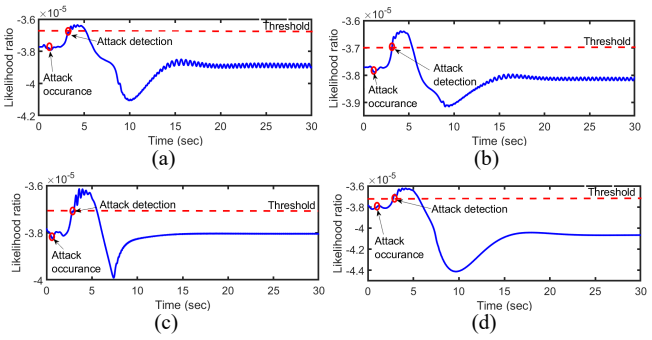

Fig. 4. Detection of SA at ES (a) base power condition. (b) 50% change in active power. (c) 50% change in reactive power. (d) 30% change in reactive power.

B. Detection of SA introduced in GS

The effectiveness of SP-PF detection technique is further evaluated, when the GS system is subjected to a SA. The SA is effective from 0.3 sec and remains applicable until 5 sec. In Fig. 5(a), the SA is initiated under base power operating condition. The likelihood ratio, a key output of the SP-PF algorithm, dynamically evolves, and when it surpasses the predefined threshold value (set as -3.72×10^{-5}) [24], the algorithm successfully detects the SA attack in the system.

To comprehensively assess the robustness of the SP-PF technique, it is further tested under different power conditions. In Fig. 5(b)-5(d), the SP-PF algorithm is evaluated under conditions, where the active power is altered to 50%, the reactive power is changed to 50%, and the reactive power is modified to 30%, respectively. Remarkably, the SP-PF technique demonstrates its capability to detect the SA under all these tested conditions, as evidenced by the outcome in the variation of likelihood ratios. Thus, this underscores the adaptability and reliability of the SP-PF detection technique in identifying anomalies and deviations induced by SAs on the governor system from normal system behavior.

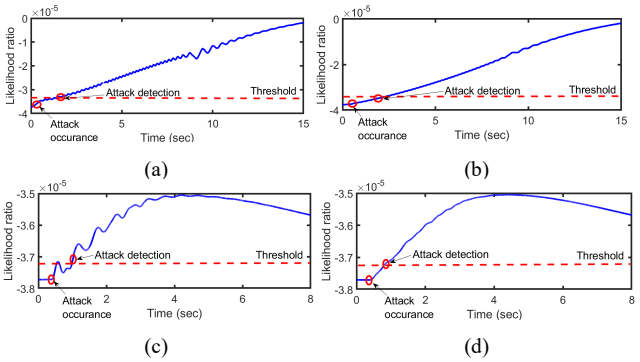

Fig. 5 Detection of SA at GS (a) base power condition. (b) 50% change in active power. (c) 50% change in reactive power. (d) 30% change in reactive power.

Also, to note unlike ES as discussed above, the variation of likelihood ratio for SA in GS, remains above the threshold scale, even after its elapse. Particularly for base power and changed active power conditions, with SA on GS, the likelihood ratio indicates a linear increase. This reaffirms the speculation from the discussion given in [25]-[26] about most vulnerability of GS than other components like ES or CB.

VI. Conclusions

In the presented study, with SA launched on ES and GS associated with the generator, the proposed detection algorithm was successfully on real-time set up. Through the combination of SP-PF, strategic allocation of particles in relevant regions and thereby resulting in reduced computational burden, the approach significantly improved the detection performance, which was demonstrated in real-time. The detection remained robust for different operating conditions and also with SA launched on either GS or ES. The approach adopted dynamically varying detection index, i.e. likelihood ratio, which on surpassing a unique threshold value indicated the SA, both for ES and GS.

Acknowledgements

This research has been performed using the ERIGrid 2.0 Research Infrastructure and is part of a project that has received funding from the European Union's Horizon 2020 Research and In-novation Programme under the Grant Agreement No. 870620. The support of the European Research Infrastructure ERIGrid 2.0 and its partner: Electrical Sustainable Power Lab (TU Delft) is very much appreciated.

Appendix

Table I: Power flow data of IEEE 9-bus power system

Bus	*Type*	*V* (pu)	P_G (MW)	Q_G ($MVAr$)	P_L (MW)	Q_L ($MVAr$)
1	SLACK	1.040 ∠0.0°	71.6	27.0	-	-
2	P-V	1.025 ∠9.3°	163.0	6.7	-	-
3	P-V	1.025 ∠4.7°	85.0	−10.9	-	-
4	P-Q	1.026 ∠ − 2.2°	-	-	-	-
5	P-Q	0.096 ∠ − 4.0°	-	-	125.0	50.0
6	P-Q	1.013 ∠ − 3.7°	-	-	90.0	30.0
7	P-Q	1.026 ∠3.7°	-	-	-	-
8	P-Q	1.016 ∠0.7°	-	-	100.0	35.0
9	P-Q	1.032 ∠2.0°	-	-	-	-

REFERENCES

[1] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems", Journal of Modern Power Systems and Clean Energy, 2022.

[2] M.M.S. Khan, J. A. Giraldo, and M. Parvania, "Attack detection in power distribution systems using a cyber-physical real-time reference model", IEEE Transactions on Smart Grid, vol. 13, no. 2, pp.1490-1499, 2021.

[3] Z. Jin, "Static and Dynamic State Estimation of Power Systems", The University of Manchester (United Kingdom), 2018.

[4] A. Saikia, and R. K. Mehta, "Power system static state estimation using Kalman filter algorithm", International Journal for Simulation and Multidisciplinary Design Optimization, vol. 7, p.a. 7, 2016.

[5] T. P. Vishnu, V. Viswan, and A. M. Vipin, "Power system state estimation and bad data analysis using weighted least square method", In 2015 International Conference on Power, Instrumentation, Control and Computing (PICC), pp. 1-5, IEEE, December 2015.

[6] M. Cosovic, and D. Vukobratovic, "Distributed Gauss–Newton method for state estimation using belief propagation", IEEE Transactions on Power Systems, vol. 34, no. 1, pp.648-658, 2018.

[7] T. Chen, Y. Cao, X. Chen, L. Sun, , J. Zhang, and G. A. Amaratunga, "A distributed maximum-likelihood-based state estimation approach for power systems", IEEE Transactions on Instrumentation and Measurement, vol. 70, pp.1-10, 2020.

[8] H. Liu, F. Hu, J. Su, X. Wei, and R. Qin, "Comparisons on Kalman-filter-based dynamic state estimation algorithms of power systems", IEEE Access, vol. 8, pp.51035-51043, 2020.

[9] A. Akrami, M.S. Asif, and H. Mohsenian-Rad, "Sparse distribution system state estimation: An approximate solution against low observability", In 2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5, IEEE, Febuary 2020.

[10] E. Vincent, M. Korki, M. Seyedmahmoudian, A. Stojcevski, S. Mekhilef, "Detection of false data injection attacks in cyber–physical systems using graph convolutional network", Electric Power Systems Research, 217, p.109118, 2023.

[11] M. Macas, and W. Chunming, "Enhanced cyber-physical security through deep learning techniques", In Proceding CPS summer school Ph. D. workshop, pp. 72-83, September 2019.

[12] Z. Huang, K. Schneider, J. Nieplocha, and N. Zhou, "Estimating power system dynamic states using extended Kalman filter", In 2014 IEEE PES General Meeting| Conference & Exposition, pp. 1-5, IEEE, July 2014.

[13] J. Zhao, L. and Mili, "Robust unscented Kalman filter for power system dynamic state estimation with unknown noise statistics", IEEE Transactions on Smart Grid, vol. 10, no. 2, pp.1215-1224, 2017.

[14] M. Ahwiadi, and W. Wang, "An adaptive particle filter technique for system state estimation and prognosis", IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 9, pp.6756-6765, 2020.

[15] R. Huang, and Y. Li, "Adversarial Attack Mitigation Strategy for Machine Learning-Based Network Attack Detection Model in Power System", IEEE Transactions on Smart Grid, vol. 14, no. 3, pp.2367-2376, 2022.

[16] M. Iloska, and M. F. Bugallo, M.F., "State-space partitioning schemes in multiple particle filtering for improved accuracy", In 2022 30th European Signal Processing Conference (EUSIPCO), pp. 2026-2030, IEEE, August 2022.

[17] Y. Cui and R. Kavasseri, "A particle filter for dynamic state estimation in multi-machine systems with detailed models," IEEE Transaction Power System, vol. 30, no. 6, pp. 3377–3385, November 2015

[18] S. Yadav, N. Kishor, S. Purwar, S. Chakrabarti, P. Raussi, P. and A. Kumar, "Real - time implementation for vulnerability of power components under SA based on sliding mode", IET Cyber - Physical Systems: Theory & Applications, 2023.

[19] K. Harrys,"WSCC 9-Bus System",2016 [ONLINE] Available at: https://harryskon.com/2016/02/28/wscc-9-bus-system/

[20] P. Kundur, N. J. Balu, and M. G. Lauby, Power System Stability and Control. New York, NY, USA: McGraw-Hill, vol. 7, 1994.

[21] P. M Djuric, T. Lu, and M. F Bugallo, "Multiple particle filtering," in 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07. IEEE, 2007, vol. 3, pp. III–1181.

[22] S. Sarkk, " Bayesian filtering and smoothing," Cambridge University Press, vol. 3, 2013.

[23] H. V. Poor, "An Introduction to Signal Detection and Estimation", New York: Springer-Verlag, 1994.

[24] Y. Boers, and P. K. Mandal, "Optimal particle-filter-based detector", IEEE signal processing letters, vol. 26, no. 3, pp.435-439, 2019.

[25] S. Yadav, N. Kishor, S. Purwar, and S. Chakrabarti, "Indirect Cyber-Physical Attack with Combined Circuit Breaker and Excitation System", In IEEE EUROCON 2023-20th International Conference on Smart Technologies, pp. 204-209, IEEE, July 2023.

[26] S. Yadav, N. Kishor, S. Purwar, P. Raussi, and S. Chakrabarti, "Switching attack modeling and vulnerability analysis of generator for dynamics study", Sustainable Energy, Grids and Networks, vol. 38, pp.101297, 2024.