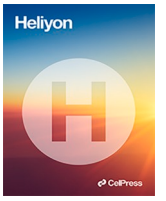
Heliyon 10 (2024) e26332

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

Detection and mitigation of coordinated cyber-physical attack in CPPS

G.Y. Sree Varshini [a,*], S. Latha [b]

[a] Research Scholar, Thiagarajar College of Engineering, Madurai 625015, India
[b] Prof/EEE, Thiagarajar College of Engineering, Madurai 625015, India

ARTICLE INFO

Keywords:
Cyber-physical power system (CPPS)
Recursive polynomial model estimator (RPME)
Coordinated cyber-physical attack (CCPA)
Adaptive model predictive controller (AMPC)
Convolutional neural network (CNN)
Support vector machine(SVM)
Random forest(RF)
K nearest neighbour (KNN)

ABSTRACT

Cyber-Physical Power System (CPPS) refers to a system in which the elements of the internet and the physical power system communicate and work together. With the use of modern communication and information technology, grid monitoring and control have improved. However, the components of a cyber system are extremely vulnerable to cyberattacks via cyber connections due to inadequate cyber security measures. Therefore, an adaptive defence strategy is required for the analysis and mitigation of the coordinated attack. The conventional approach of using an offline controller requires tuning for changes in the operating conditions of the system, which is inappropriate for the modern CPPS. To counter the coordinated attack, a framework that integrates STATCOM based Adaptive Model Predictive Controller with RPME and time delay compensator is proposed. This paper addresses attack impact, detection, and mitigation methods in CPPS. In both time domain and frequency domain simulations the case studies are conducted for three distinct situations namely physical attack, cyberattack, and coordinated attack. Convolutional Neural Network (CNN), Support Vector Machine (SVM), Random Forest (RF), and K Nearest Neighbour (KNN) are four data-driven methods used for the detection of anomalies in PMU measurement data. Simulation studies show that CNN performs better in anomaly detection than other classifiers based on assessed performance metrics. For coordinated attack mitigation the proposed STATCOM based Adaptive Model Predictive Controller with RPME quickly recovers the system than the STATCOM based conventional lead-lag controller. The efficacy of the proposed strategy is validated on the WSCC 3 machine 9 bus system.

1. Introduction

The main concern for the stability of the power system is the low frequency inter-area mode of oscillation that results from power transmission in weak tie lines with insufficient regulatory devices [1]. Therefore, the blackout of the system will result from the poorly dampened inter-area mode of oscillation. For example, system blackout events happened in India on July 30, 2012 and the USA on the 2nd and July 3, 1996, and in the Eastern U.S. on the August 14, 2003. Power outages can cause a nation's economy, politics, and social well-being to suffer. Despite having various protection mechanisms, power systems can experience malfunctions that cause cascading events that could even result in a blackout. The power system operators and control system researchers have focused on wide area control (WAC) for the past two decades to preserve the global system stability through monitoring the wide-area power system

* Corresponding author.
E-mail addresses: gysreevarshini90@gmail.com (G.Y. Sree Varshini), sleee@tce.edu (S. Latha).

https://doi.org/10.1016/j.heliyon.2024.e26332
Received 3 August 2023; Received in revised form 11 February 2024; Accepted 12 February 2024
Available online 19 February 2024

dynamics with the help of synchro phasor measurement technology. Phasor data concentrators (PDCs) receive data from GPS-synchronized PMUs dispersed throughout the grid. PMUs give a dynamic view of the smart grid in real-time, allowing for real-time protection and control, and they improve the system's situational awareness. This inspired the authors to create a WAC framework using PMU measurement to address CCPA.

The merging of cyber and physical systems [2] yields a brand-new digital technology called a "cyber-physical system". Integrated communication and information systems are referred to as "cyber systems." The man-made systems controlled by physics regulation are defined as "physical systems". Cyber systems collect data from physical systems using sensors and feed that data back as a control signal to achieve common objectives. In addition to the control devices with the tight integration of information and communication technology, the existing power system is evolving into CPPS. Cyber-attack is the major concern in today's smart grid. In recent years grids have become more prone to cyber-attack-like events [3] that occurred in the western Ukraine power grid in December 2015, a malware attack in a Saudi Arabia oil refinery in 2017, a Denial of Service (DOS) attack on German power utility in 2012, Kudankulam nuclear power plant was attacked with malware on October 30, 2019. Professional hackers, hostile insiders, and organized criminal gangs are all capable of introducing a cyber-attack. Energy theft, widespread blackouts, or the destruction of vital infrastructure are just a few of the serious effects that cyber-attacks can have on the grid. Industroyer, a recently identified malware, may target numerous communication protocols, including IEC 60870-5-101, IEC 60870-5-104, and IEC 61850, and is capable of taking control of substation switches and breakers. To combat the damaging impacts on the infrastructure of the increasingly complex cyber-attacks on CPPS, detection and mitigation methods are required.

Cyber security is essential not only for protecting sensitive information but also for ensuring the stability and reliability of critical infrastructure and services in our increasingly digital world. The growing use of digital technology and communication networks in the operation and management of electrical grids raises serious concerns about cyber security in the power grid. To preserve its dependability, availability, and resilience, the power grid must be protected against cyber-attacks. The process of maintaining cyber security in the electrical grid calls for regular monitoring, adaptation to changing threats, and a dedication to safeguarding vital infrastructure. In addition to hurting the supply of electricity, a successful cyber-attack on the power grid might also damage public safety and national security. So, it is crucial to have strong cybersecurity measures against the attack. In this article an adaptive defence strategy namely STATCOM based AMPC with RPME is used to counter the coordinated attack on the WAC application of CPPS.

When an attacker tries to stop or exploit the services from providing a necessary action, it is called a "DoS attack." By making communication with a device impossible or causing the device to crash, DoS attacks can delay time-critical messages and inflict a full denial of service [4]. Voltage support devices based on damping controllers depend mainly on PMU devices [5] to receive wide-area control signals for compensating the reactive power in the transmission line and enhancing stability during contingency. PMU uses a wide area network for communication with other devices like PDC and control centres. By sniffing communication networks, attackers collect information and utilize it to plan attacks. Thus, the geographically dispersed substation has limited network protection which makes the attackers to easily manipulate the signal and cause disturbance to the smart grid. Therefore, when a time delay attack occurs on the measurement signal of the FACTS device, the attacked signal is given to the STATCOM which in turn applies a delayed control signal. As time progresses, it results in loss of synchronism which eventually causes instability and collapse. Therefore, CPPS requires an adaptive defence approach to protect the grid and assets.

In the past decade, few research has been carried out to analyze the effect of coordinated cyber-physical attacks on smart grids. CCPA cause a higher impact on the smart grid than individual attack does. Therefore, investigation and analysis of coordinated attack is indispensable in CPPS study. Prasanta et al. [6] analyzed the impact of CCPA using generation cost variation and nodal prices between pre-attack and post-attack scenarios of different IEEE test systems in electricity market applications. Jun et al. [7] analyzed CCPA considering false overload event and evaluated its effect using evaluation indices of generator output cost, load reduction cost, and overloaded lines. There is no countermeasure technique addressed in the proposed work. Wenjie [8] et al. proposed different attack strategies in smart grids and analyzed their vulnerabilities. Jiwei et al. [9] investigated coordinated cyber-physical attack effects in the IEEE 14 bus system and adopted the big M method to solve the optimisation issue. The author did not describe the defence approach against the attack in research work. Arman Sargolzaei [10] described the prevention of time delay attacks using a controller by estimating the delay with model reference control and the least mean square minimization technique. In Ref. [11] the author investigated cyber security of the power grid, from component-level vulnerability assessment to system-level impact analysis. Bo Chen et al. [12] discussed the impact of cyber-attack on transient angle and voltage stability with two voltage devices namely SVC and STATCOM in 8 bus test system using DSA tools. Aoron [13] et al. proposed an approach for cyber-physical interaction study in wide area control applications. Siddharth Sridhar et al. [14] highlighted the attack impact targeted at voltage control devices (FACTS) using a sensitivity analysis technique. In Ref. [15] the author discussed the cyber-attack on SVC (Static VAR Compensator) measurement data and its impact on transient voltage and angle stability in IEEE 39 bus system using DSA tools. Narayan Bhushan et al. [16] proposed a multi-label classification method based on deep learning techniques to identify coordinated attacks and tested it in IEEE 123-node and 240-node real distribution systems. To boost the resilience of the power grid against coordinated attacks, a defensive technique using a level optimisation model based on post-allocated Distributed Generators (DGs) is proposed by Huihui et al. [17]. In Ref. [18] the author introduces a novel real-time FDIA identification strategy based on a deep learning-based state forecasting model, followed by a novel intrusion detection method utilizing the error covariance matrix in the IEEE 14 bus system. With an additional control loop to protect against denial-of-service (DoS) attacks, the study [19] suggests resilient event-triggered LFCs for CPPSs. The author described a resilient event-triggered communication system to lessen the additional control loop's reliance on communication resources during denial-of-service attacks. The study then builds a novel switching LFC system model, which in contrast to existing event-triggered LFC systems integrates the resilient event generator into an extra control loop when subject to DoS attacks. One-area and two multi-area CPPS are used to demonstrate the viability of the suggested method. From the past research work, it is inferred that

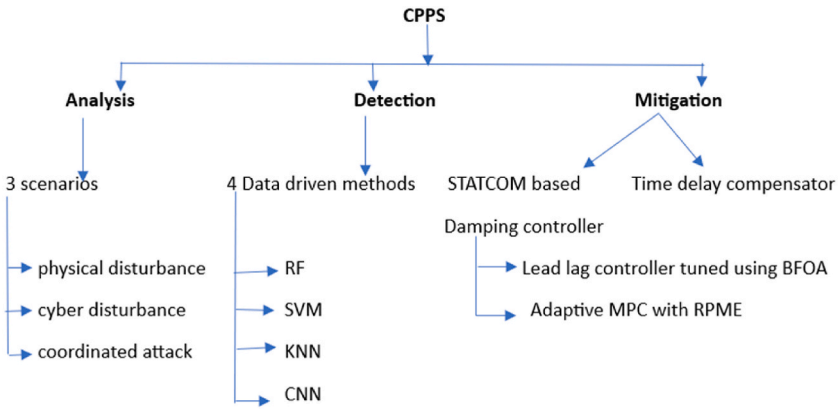


Fig. 1. Overview of Proposed work.

most of the studies considered only a single attack (either physical or cyber-attack) but lacked analysis of coordinated attacks in wide area control applications. In this research work, it is assumed that the adversary's goal is to inject the time delay in the communication signal of the STATCOM based damping controller, to cause instability and sabotage to the grid. Therefore, an adaptive defence technique was developed to thwart CCPA in the modern CPPS. Simulation results are obtained and evaluated with three different scenarios namely physical disturbance, cyber disturbance, and coordinated cyber-physical attack.

When the dynamics or parameters of the system change, adaptive controllers can automatically update their parameters to match. As a result, they are more resistant to changes in the controlled system without requiring retuning. Since the CPPS is a complex system of nonlinear dynamics or time-varying characteristics benefits most from adaptive control. Systems can continue to operate reliably and satisfactorily even in the face of errors or failures with the aid of adaptive controllers. But controllers that are tuned offline shows poor performance when operating condition changes. When new data is available RPME updates its estimate making it suitable for applications requiring timely information. In situations where noisy or erratic estimates are undesirable, recursive estimators frequently give smoother estimates than non-recursive approaches. Moreover, it can offer low-latency reactions to changes in the system since it updates their estimates continually. This is beneficial for quick decision-making on control operations. Therefore, the integrated framework of both the adaptive controller with recursive estimator and compensator leads to the implementation of an adaptive defence strategy against coordinated attack in CPPS.

The contribution of this paper is summarized as follows:

(i) The WSCC system is modelled as CPPS with hybrid simulation using SIMULINK and SIMEVENTS.
(ii) The system is simulated with a physical attack (three phases to ground fault) and cyber-attack (time delay attack) and its impact is addressed.
(iii) Designed a STATCOM based conventional damping controller and STATCOM based AMPC damping controller with RPME for online identification and estimation of power system parameters during contingency and also to mitigate the oscillation for the improvement of wide-area stability.
(iv) Detection of cyber and physical disturbance using data-driven methods and also designed time delay compensator for mitigation of time delay effect.
(v) In frequency domain analysis, welch power spectral density estimate is used to analyze different disturbance responses of the system.

Thus, the research work involves coordinated attack impact analysis, detection, and mitigation in a time domain simulation environment. Section 2 and 3 describes the mathematical modelling of CPPS and communication network modelling using SIMEVENTS respectively. Section 4 describes the properties of cyber-physical attacks in CPPS. Section 5 presents the design of a conventional damping controller for STATCOM. Section 6 explains the design of the AMPC damping controller for STATCOM with RPME. Section 7 discusses the time delay compensator. Section 8 describes the detection of the anomaly using data-driven methods. Section 9 analyses the time and frequency domain simulation results. Finally, the Conclusion is given in section 10. An overview of the proposed work is shown in Fig. 1. An illustration of CCPA detection and mitigation is shown in Fig. 22.

2. Mathematical modelling of CPPS

Consider the WSCC system as CPPS with a STATCOM device. The wide area control signal (speed deviation) is obtained through the communication channel and modulated by the FACTS device for control action to take place. The mathematical equation of the physical system (power system) can be represented using (1) and (2)

$$y = h(x,u), \dot{x} \in F_P(x,u) \tag{1}$$

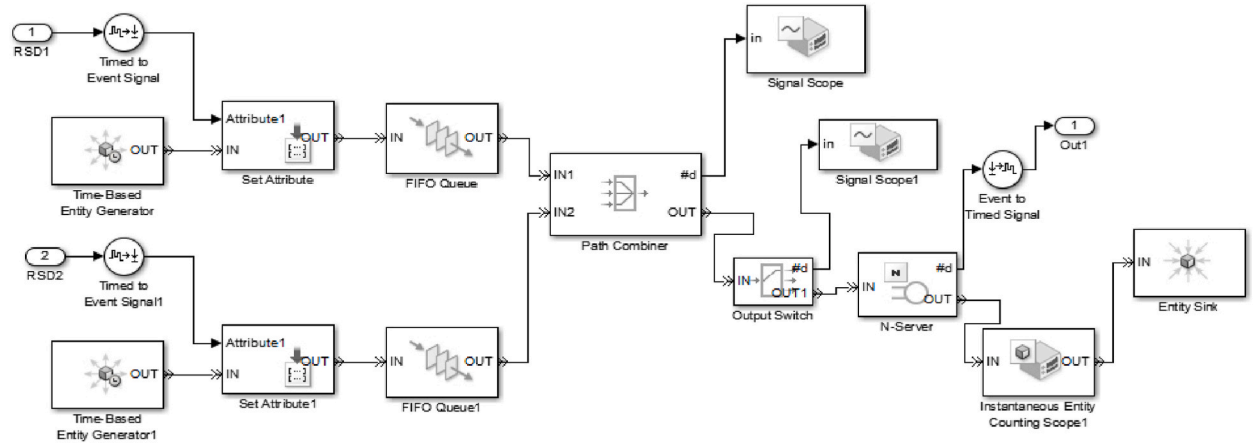


Fig. 2. Discrete event based modelling of communication network.

$$(x, u) \in C_P \subset \mathbb{Z}^{n_P} \times \mathbb{Z}^{m_P} \tag{2}$$

Where, $\mathbb{Z}^{n_P}$ - Euclidean space for state space
$u \in \mathbb{Z}^{m_P}$- input signal for the physical system,
$y \in \mathbb{Z}^{r_P}$ - output of the physical system
h - output function
x - state of the physical system.
The mathematical equation of the cyber system (communication network) can be represented using (3) and (4),

$$\zeta = K(\eta, \gamma), \eta^{+} \in G_C(\eta, \gamma), \tag{3}$$

$$(\eta, \gamma) \in D_C \subset \Upsilon \times \gamma \tag{4}$$

$\eta \in \Upsilon$ - state of the cyber system
$\mathbb{Z}^{n_C}$ - Euclidean space for the state space,
$\gamma \in \vee \subset \mathbb{Z}^{m_C}$ - input signal for the cyber system,
$\zeta \in \mathbb{Z}^{r_C}$ -cyber system output defined by the function K.
K – Function of input γ and the state η.
Information transferred over the communication network at time instant,
$\{\tau_i\}_{i=1}^{p^*}, p^* \in \mathbb{N} \cup \{\infty\}$ satisfying,

$$T_n^{*min} \leq \tau_{i+1} - \tau_i \leq T_n^{*max} \quad \forall \; i \; \{1, 2, ..p^* - 1\}$$

T_n^{*min}, T_n^{*max} - constants satisfying the following constraints

$$T_n^{*min}, T_n^{*max} \in [0, \infty]$$

$$T_n^{*min} \leq T_n^{*max}$$

Where, p^* - no. of. transmission events
T_n^{*min}, T_n^{*max} - minimum and maximum time between the transmission events.
The mathematical model of the communication network are represented in (5) and (6),

$$\dot{\tau_n} = 1, \dot{m_n} = 0 \;\text{ when } \tau_n \in \left[0, T_n^{*max}\right] \tag{5}$$

$$\tau_n^{+} \in \left[T_n^{*min}, T_n^{*max}\right],$$

$$m_n^{+} = v_n \quad \text{when } \tau_n \leq 0 \quad . \tag{6}$$

The continuous and discrete dynamics of CPPS are represented in (7)-(9)

$$\dot{\nu} \in F_I(\nu, q) \text{ when } (\nu, q) \in C_I \tag{7}$$

$$\nu^{+} \in G_I(\nu, q) \text{ when } (\nu, q) \in D_I \tag{8}$$

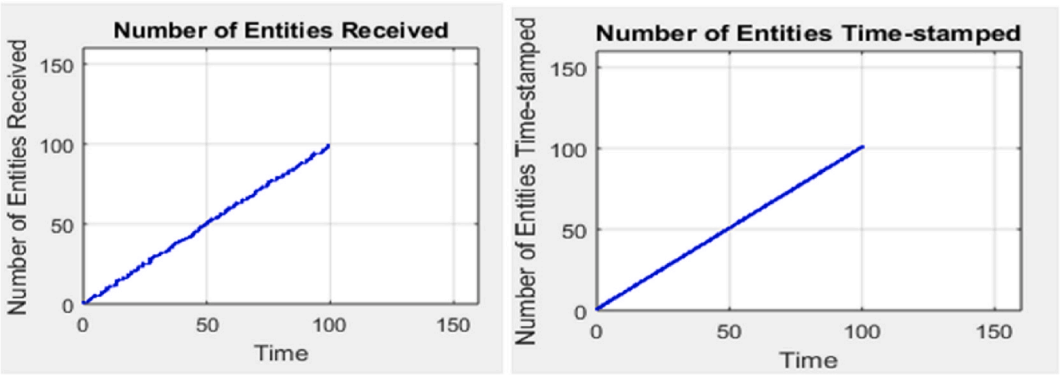


Fig. 3. (a) Number of entities received at the destination; (b) Number of entities which is time stamped.

$$\beta = \varphi(\nu) \tag{9}$$

where ν -state, q-input signal, β –output signal, F_I -continuous dynamics on C_I, G_I -discrete dynamics on D_I.

3. Communication network modelling using SIMEVENTS

The CPPS is modelled using SIMEVENTS and SIMULINK in MATLAB. SIMEVENTS are used to model the communication network for transmission of signal from sensor to controller [20,21]. SIMULINK is used to model the physical dynamics of the power system. Thus, the hybrid model is used to convert continuous signals to discrete event signals and uses packet communication using entities. Therefore, it involves both time-based and discrete event-based modelling. From Fig. 2 it is inferred that the rotor speed deviation signals from generators 1 and 2(RSD1 and RSD2) are time domain signals which are converted to discrete event signals using time to event signal block. To generate random packets or entities, a time-based entity generator is used with an exponential distribution of mean = 100. The attributes are attached to the packets using a set attribute block. FIFO queue are set to fix capacity of 25 each. Entities from different paths are merged using a path combiner and out switch block enables the routing of entities to the final destination. The server serves the entities for a period of time where it is converted again to a time domain signal to feed into the damping controller. Fig. 3(a) and (b) represent received entities at the destination of the communication network and time-stamped entities respectively.

4. General properties of Cyber Physical Attack in CPPS

Attacks on power systems that intentionally manipulate or compromise both its physical and cyber components are known as “cyber-physical attacks”. Power outages, physical infrastructure damage, and risks to public safety are just a few of the serious effects that these attacks may have. Some of the properties of Cyber Physical Attack on CPPS are:

1. Cyber and physical layer dependencies: Digital control systems (the cyber layer) and physical processes (the physical layer) are tightly integrated in CPPS. Attacks on one layer may have a direct impact on the other due to their interdependence.
2. Attacking covertly: Cyber-physical attacks are frequently created to be covert, making it challenging to identify them. Attackers could try to have a low profile to avoid being immediately discovered, allowing them to acquire information or do harm over an extended period of time.
3. Stage-Based Attacks: Cyber-physical attacks frequently have several steps or stages. Attackers may get access to control systems through initial cyber invasions, which they can later use to cause physical harm or disruption.
4. Distance Access: Since many cyber-physical attacks are carried out remotely, attackers can breach the infrastructure without being in the immediate area. This can make attribution and response more difficult.
5. Operations disruption: Cyber-physical attacks in CPPS frequently aim to interfere with regular power grid operations. Attackers may want to create risky situations, equipment damage, or power disruptions.
6. Cascading failures: The electrical system may experience cascade failures as a result of disruptions brought on by cyber-physical attacks. For instance, a substation attack may result in overloads or voltage instabilities in other grid areas.
7. Confidentiality and Deception: To hide their identity or lead investigators astray, attackers may employ several strategies. This may involve the use of false flags, obfuscation strategies, and proxy servers.
8. Motivations: Attackers may be inspired by a number of motives, including monetary gain, political gain, espionage, or simply the desire to harm infrastructure.

5. Design of STATCOM based lead lag damping controller

STATCOM is a compensating device [22] which will inject or absorb the reactive power according to the system’s operating

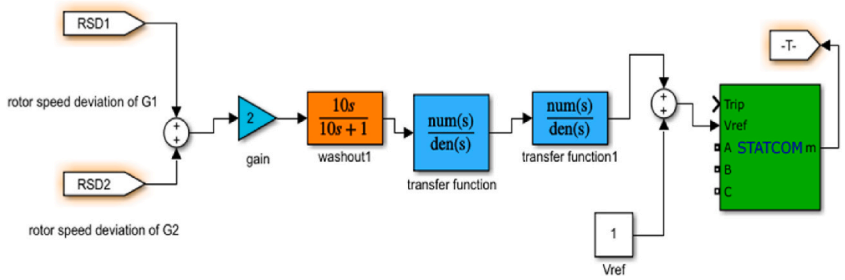


Fig. 4. The SIMULINK model of lead-lag damping controller.

Table 1
Parameters of BFOA and lead-lag controller.

Parameters of BFOA	Parameters of Lead lag controller
• No. of bacterium, s = 10 • search space dimension, p = 5 • Swim length, $N_s = 6$ • chemotactic steps, $N_c = 6$ • No. of reproduction steps, $N_{re} = 6$ • No. of bacteria reproductions per generation, $S_r = s/2$ • No. of elimination dispersal process, $N_{ed} = 4$.	• Gain, K = 2 • Washout = 10s • Phase compensation $T_1 = 0.3362$, $T_2 = 0.2684$. $T_3 = 0.3649$, $T_4 = 0.2598$ • $V_{ref} = 1$

condition but will not dampen out the inter-area mode of oscillations occurring due to physical disturbance. Therefore, a supplementary damping controller is designed to dampen the oscillations [23,24]. The structure of the damping controller consists of three block namely the gain block, washout block and phase compensation block. The function of the gain block is to dampen the oscillation. The function of the washout block is to permit oscillating signals from the input signal to pass through unaltered. The phase compensation block provides the phase lead characteristics to account for the phase lag that occurs between the input and output signals. Whenever oscillation occurs due to natural or man-made disturbance, the power system parameters (power angle, rotor speed, tie-line power, bus voltage) will deviate from the nominal value. In the WAC application, speed deviation is chosen as an objective function which is efficient in damping the inter-area mode of oscillation. Moreover, it is independent of the operating point whereas the power angle, the real power signal is dependent on the steady state equilibrium point of the system. The STATCOM device is connected at the middle point of the transmission line near bus 5, to achieve equal compensation on both sides of the system. SIMULINK model of the Lead lag damping controller is shown in Fig. 4. PMU Simulink block is connected near bus 5 of the WSCC system to acquire the PMU data.

$$V_{st} = \Delta V_{st} + V_{ref} \tag{10}$$

equation (10) implies that the desired value of compensation is obtained by adding change in STATCOM voltage (ΔV_{st}) and the reference voltage (V_{ref}).

The minimization objective function is shown in (11),

$$J = \int_{t=0}^{t=t_{sim}} (\Delta\omega_1 + \Delta\omega_2)t.\, dt \tag{11}$$

Subject to,

$$K_i^{min} \le K_i \le K_i^{max}$$

$$T_{1i}^{min} \le T_{1i} \le T_{1i}^{max}$$

$$T_{2i}^{min} \le T_{2i} \le T_{2i}^{max}$$

$$T_{3i}^{min} \le T_{3i} \le T_{3i}^{max}$$

$$T_{4i}^{min} \le T_{4i} \le T_{4i}^{max}$$

Thus, the objective function is to minimize the speed deviation of the rotor with respect to time. The remote signal (Δω1, Δω2) of generator 1 and 2 is taken as a wide area signal for the damping controller input.

A modern global optimisation method of relevance for distributed optimisation and control is the Bacterial Foraging Optimisation Algorithm (BFOA). BFOA takes its cues from bacteria's chemotaxis behaviour, which involves moving towards or away from particular

Table 2
Parameters of AMPC and RPME.

Parameters of RPME	Parameters of AMPC
• Model structure: ARX • No of parameters in A(q) = 3 • No of parameters in B(q) = 3 • Parameter covariance matrix = 1 • Sample time = 0.5 • Estimation method: forgetting factor • Forgetting factor:0.01	• Prediction horizon = 4, • Control horizon = 2, • Ts = 0.5, • Weight of manipulated variable = 5.4595, • Weight of output variable = 0.0183 • Optimal cost = 0.004034

signals in response to chemical gradients in the environment. An imitation of the biology that underlies *E. coli*'s foraging strategy is made, and it is then used as the basis for a straightforward optimisation technique. BFOA is a nature-inspired algorithm which is employed for tuning damping controller parameters due to its ease of implementation and simplicity. Parameters of BFOA and lead-lag controller are given in Table 1.

6. Design of STATCOM based AMPC damping controller with RPME

Power system parameters are time-varying and nonlinear nature therefore RPME with ARX model is proposed to estimate time variant parameters during plant operation. RPME estimates discrete-time ARX model coefficients (A(q), B(q)) of the model and converts it into a state space model using a model type converter. Thus, the online identification and estimation of model parameters at each sampling instant in an ARX form are computed by RPME. This method can also be used to estimate parameters during large disturbance conditions and also provide smooth estimation performance. The input for the estimator is field voltage and the output is rotor speed difference between generators 1 and 2. The state space model of the WSCC system under time delay attack is represented in (12) and (13),

$$\dot{\hat{x}}(t) = A\hat{x}(t) + BU(t) + k(Z(t) - \hat{Y}(t-\hat{\tau})) \tag{12}$$

$$\hat{Y}(t) = C\hat{x}(t) \tag{13}$$

The STATCOM device is represented by a discrete-time auto-regressive polynomial model with the following form as given in (14)-(16)

$$A\left(q^{-1}\right)y(t) = \sum_{i=1}^{mu} B_i q^{-1} u_i(t - mk_i) + e(t) \tag{14}$$

$$A\left(q^{-1}\right) = 1 + a_1 q^{-1} + a_2 q^{-2} + a_3 q^{-3} \ldots + a_{n_a} q^{-na} \tag{15}$$

$$B\left(q^{-1}\right) = b_0 + b_1 q^{-1} + b_2 q^{-2} + b_3 q^{-3} \ldots + b_{n_b} q^{-nb} \tag{16}$$

The generic version of the recursive identification algorithm is provided by equation (17)

$$\hat{\theta}(t) = \hat{\theta}(t-1) + K(t)[y(t) - \hat{y}(t)] \tag{17}$$

Gain $K(t) = M(t)\psi(t)$ which determines how much prediction error affects the estimated parameter and it is computed using (18) and (19). $\psi(t)$ represent regression parameter and computed based on previously measured input and output values.

$$M(t) = \frac{p(t-1)}{\Omega + \psi(t)^T p(t-1)\psi(t)} \tag{18}$$

$$\psi(t) = [y(t-1)y(t-2)\ldots y(t-n) \quad u(t-1)u(t-2)\ldots u(t-n)]^{\mathrm{T}} \tag{19}$$

Ω represent forgetting factor and its value is shown in Table 2.

$M(t)$ is obtained by minimizing below constraint shown in (20)

$$\sum_{k=1}^{t} \Omega^{t-k} \left(y(k) - \hat{y}(k)\right)^2 \tag{20}$$

Estimated parameter $\hat{\theta}(t)$ recursively computed by equation (21)

$$\hat{\theta}(t) = \hat{\theta}(t-1) + K(t)\left[y(t) - \hat{\theta}^T(t-1)\psi(t)\right] \tag{21}$$

When a plant's characteristics are nonlinear or change over time, adaptive MPC controllers modify their prediction model during runtime. To implement AMPC, first we design a classic model predictive controller for the control system's nominal operating circumstances and then update the plant model. The plant model and nominal circumstances stay unchanged after updating across the

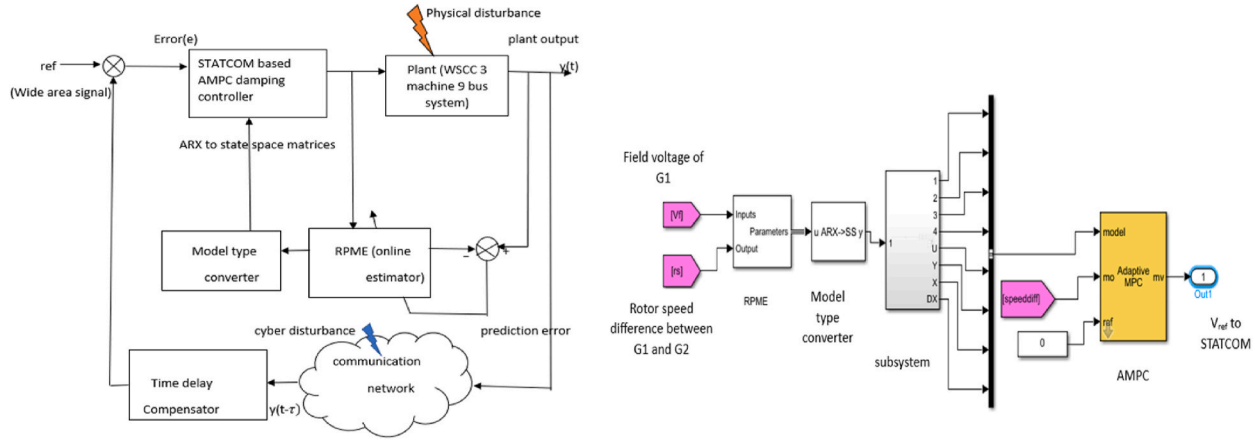


Fig. 5. (a) Block diagram of proposed technique; (b) SIMULINK model of AMPC damping controller with RPME.

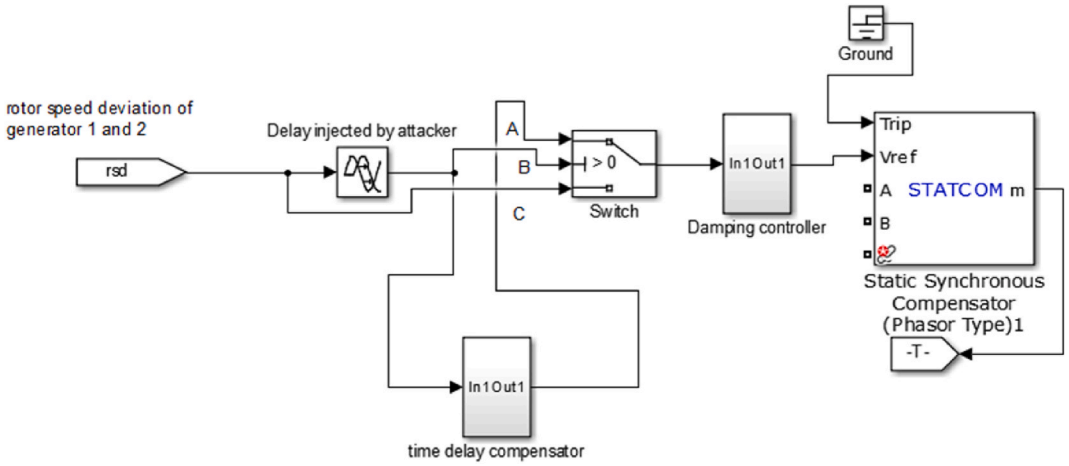


Fig. 6. SIMULINK model of time delay compensator and STATCOM based damping controller.

prediction horizon. The prediction model of adaptive MPC controllers is changed in real time in response to nonlinear or time-varying plant characteristics. The suggested adaptive control method can handle significant disturbances and changes that have occurred in the system without the need for controller retuning and is applicable to a wide range of operating circumstances. It can handle complexity traits like high dimensionality, time delay, unmodeled dynamics, system parametric uncertainties. The drawback of MPC is that fixed model parameters make its predictions irrelevant to the current state of the system when the plant operating point changes and also results in poor prediction accuracy. Therefore, by calculating plant parameters online with RPME, AMPC adjusts the plant model coefficients at each control interval to calculate the control signal. As soon as the plant parameters have been assessed online, AMPC gives an optimal control signals and applies them to the plant at each control interval to minimize output deviation from the desired value. Thus, the optimisation problem is described as a reference tracking problem and solved with AMPC to produce modified variables for the plant at each control interval. The input signal for STATCOM is composed of the sum of the AMPC damping controller signal and the fixed reference signal. By modulating the control signal input to STATCOM's reference point through an external AMPC damping controller, inter-area oscillation is stabilised. To accurately predict the plant parameters, a sampling time of 0.5 is used. The block diagram of the proposed technique is shown in Fig. 5(a) and the Simulink model is given in Fig. 5(b). Parameters of AMPC and RPME are given in Table 2.

Obtained State space matrices of controller model by RPME,

$$A = \begin{bmatrix} 4.05 & 1 & 0 \\ -5.411 & 0 & 1 \\ 2.361 & 0 & 0 \end{bmatrix} \quad B = [-0.1421 \quad 0.2226 \quad -0.08083], C = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, D = [0]$$

Estimated states of AMPC controller is

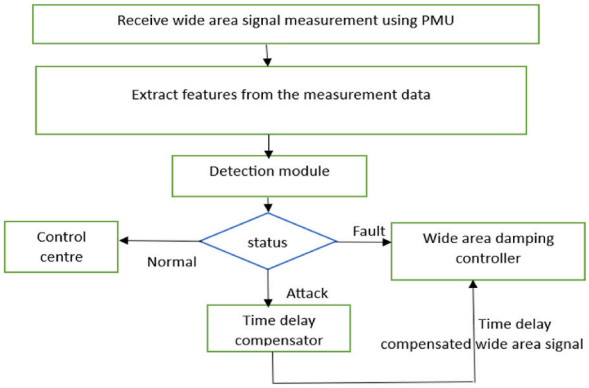


Fig. 7. Flowchart for detection of physical and cyber disturbance.

$$\widehat{\theta}(t) = \begin{bmatrix} 0.07002 & 0.3256 \\ 0.2025 & 0.8802 \end{bmatrix}$$

7. Design of time delay compensator

The attacker may inject the time delay in terms of milliseconds or even at a lower magnitude to execute the attack stealthier and unnoticeable by conventional sensors. Therefore, calculating the delay and compensating for the effect at a faster rate is essential for the system to prevent any catastrophic event. To compensate for the time delay that occurred, the compensator is designed using a one-dimensional adaptive lookup table. The advantage of the look-up operation is the speed in retrieving data from the table corresponding to the delay that occurred. This eliminates calculating the number using a trigonometric function or algorithm. In the Simulink diagram, the switch has three positions namely A, B, C. The control port is B and the data port is A and C. If time delay disturbance occurs, it will be sensed by port B and it switches to data port A where the delayed signal is compensated by a time delay compensator. If there is no cyber disturbance then the control port B switches to data port C which bypasses the compensator. Fig. 6 represents the SIMULINK model of the time delay compensator and STATCOM based damping controller.

8. Data driven method of anomaly detection

Machine learning (ML), a subset of artificial intelligence, is the collective term for all techniques and algorithms that allow computers to automatically learn from vast information using mathematical models [25–29]. Trends and interest in applying machine learning and deep learning-based anomaly detection to handle cyber-attack challenges have increased recently. Numerous ML and DL-based methods have been published by researchers to improve the ability of intrusion detection systems to recognise malicious attempt. Artificial intelligence methods can deliver quick and precise information-driven solutions for both predicting and controlling. Machine learning is a method of information analysis that uses learner interaction to program a machine to perform specific tasks. The flowchart for the detection of anomalies using the data-driven method is shown in Fig. 7. Hyper parameter tuning is required when determining parameters using ML or DL techniques. Before a model is trained, its configuration parameters are given. They have substantial influence over the model's performance and have control over several training process variables. The model is trained and analyzed for various hyper parameter settings (e.g.: No. of neighbours in KNN, regularization parameter C in SVM, tree depth in RF, filter size and learning rate in CNN) and then the performance metrics are evaluated. We shall take into account the hyper parameter that provides the optimum performance. After which a trained model is deployed.

8.1. SVM

By classifying data points as either normal or anomaly depending on how close they are to a decision boundary, SVM can be used to discover anomalies in data sets. It can identify an ideal hyperplane that maximises the difference between normal and anomalous data points. Configure the SVM to identify a hyperplane with a maximum margin around the normal instances and a minimum number of support vectors (the data points that define the margin). Calculate the distance from the decision boundary of the trained SVM model to each data point in the test set, which includes both normal and anomalous cases. Smaller distances or negative distances signify that a data point is closer to the decision border and may be an anomaly, whereas large distances from the decision boundary show that a data point is comfortably inside the typical region. Metrics are used to evaluate the SVM model's performance in detecting anomalies. To enhance the performance of the SVM model, repeat the process iteratively by changing the model's hyper parameter. The SVM method can be used to improve both its accuracy and efficacy by correctly predicting the normal and attack classes. The SVM tries to define a hyper-plane that separates data points in an S-dimensional subspace. The kernel function is used to first map a low-dimensional input vector into a high-dimensional feature space. An ideal maximum marginal hyper-plane is created using the support vectors and acts as a decision boundary. In this classifier, the regularization parameter is 1 with a degree of 2 is used.

The mathematical formulation of the classification approach is shown in (22)

$$f(m,v)=\sum_{i=1}^{S} v_i x_i(m)+\mathbb{K} \tag{22}$$

v_i defines the prediction parameters in S dimension space. The data distribution and classification variables together determine $\mathbb{K}$ using (23)

$$k(r,z)=\exp\left(-\Theta||r-z||^2\right) \tag{23}$$

In order to give identical data points in a dataset, this function is used in conjunction with SVM.

8.2. KNN

KNN, one of the simplest supervised machine learning algorithms, classifies a particular data sample using the concept of "feature similarity". It determines the class label by comparing the instance to its nearest neighbour in the training set [30]. To categorise a new sample, a KNN classifier searches the training set for k samples that are most similar to the test sample. By grouping query points according to how near they are to the points in a training data set, new points can be classified quickly. It can determine a sample's identity by measuring how far a sample is from its neighbours. The kth parameter of the KNN method determines how well the model performs. The model might be prone to over-fitting if k is quite low. If the k value is selected with an extremely wide range, the sample case might not be accurately identified. As a result, the k value should be properly chosen. The majority vote of an attack's neighbours decides whether it belongs in the class with most members among its k closest neighbours. In this classifier, three number of neighbours with cosine metric is used. The degree of similarity between data points is assessed using the Euclidean distance metric. Either by experimenting or using domain knowledge set the value of k while making prediction. Determine the separation between each data point in the test set and its 'k' nearest neighbours in the training set. The distance to the 'k' nearest neighbour is commonly used to determine the anomaly score for each test data point. Therefore, for each data point in the test set, get the distance to the 'k' nearest neighbour. Metrics such as precision, F1 score, and accuracy can be used to evaluate the KNN model's performance in terms of anomaly detection. The performance of the model can be enhanced by modifying distance metric and hyper parameters like 'k'. Using Euclidean distance, the classification algorithm refreshes the data by calculating the distance between each sample in a dataset. For k number of training data set with m attributes $\{x_{i1},x_{i2},\ldots x_{im}\}$ and testing data set $\{y_1,y_2,\ldots y_m\}$ with label l_i where iϵ[1,k]. The Euclidean distance between the training and testing data set is computed using (24)

$$d(x,y)=\sqrt{\sum_{j=1}^{k}\left(x_j-y_j\right)^2} \tag{24}$$

8.3. RF

In an effort to rectify the overfitting of a single decision tree, the random forests technique combines several decision tree classifier models [31,32]. The random forest method constructs a decision tree from a sample of data, forecast each one, and then votes on the best outcome. A random forest R is composed of the k decision tree model. Each decision tree makes a different prediction for the input testing data before a simple majority vote is utilised to determine the outcome. In order to categorise a new object x, RF aggregates the votes from all of the decision trees(d) in the forest(r). The projected class of x decided by the tree is the class that frequently appears in the random forest and receives the majority of votes. According to the definition of the simple majority voting formula shown in (25)

$$r(X)=argmax\sum_{i=1}^{d} I(r_i(X)=Y) \tag{25}$$

Where $X=(x_1,x_2,\ldots x_p)^{\mathrm{T}}$, X is the dataset with 'p' number of samples.

Individual tree projections are made individually, whereas the RF prediction is made by majority vote. The prediction accuracy is improved by averaging the outcomes of many DT classifier fits on various subsamples of the data set. Instead of focusing on the most crucial characteristic when dividing a node, it seeks for the best feature among a selection of random features. In this classifier, 10 trees with a maximum depth of 12 are considered. Utilizing the ensemble of decision trees in Random Forest, anomaly detection can be accomplished by locating data points that differ from the pattern shown in the training data. First Set the Random Forest model's hyper parameter including the number of trees and tree depth to have an ensemble of decision trees. Then determine the average distance (similarity) between a data point and each tree in the forest. Due to the differences between anomalies and the normal data, poorer closeness scores are expected for anomalies. Utilize criteria like precision, accuracy, and F1 score to evaluate the Random Forest model's performance for anomaly identification. Repeat the process by modifying the Random Forest model's hyper parameter to enhance the model's performance.

8.4. CNN

Stacks of convolutional and pooling layers, an input layer, a fully connected layer, and a SoftMax classifier make up the CNN structure [33,34,35,36,37]. CNN is a useful method for processing time series data because time series have a strong 1D locality that convolutions can retrieve. There are many filter and convolution layer counts that can be utilised, depending on the input dimension and processing power of the data. Each neuron in the fully connected layer uses a 1-D data to produce its score, which is calculated using the following equation (26)

$$y_i = \sum_{j=1}^{m} w_{i,j} x_j + b_s \tag{26}$$

Where y_i is the fully connected layer output in the ith neuron, m is the 1-D input data length (x), $w_{i,j}$ is the weight of neuron between the jth input value and ith neuron and b_s is the bias. After computing the above value of y_i, it will use an activation function to send the value to the associated units in the higher layer to see how much it affects the prediction of the following step. The activation function is provided in equation (27)

$$a_i = f(y_i) = \max\ (0, y_i) \tag{27}$$

The output of the activation function $f(y_i)$ is a_i. Rectified Linear Unit (ReLU) is used as the activation function which prevents overfitting problems. By linking each neuron to its neighbours' neurons, CNN overcomes the drawbacks of conventional neural networks. The convolution operation will be carried out with the input 2-D data employing a filter with the same size receptive field after the one-dimensional time series data have been converted to two-dimensional data. Then the features are extracted from the input by a 2-D convolution layer. The greatest value of the field covered by the pooling filter will be selected by the pooling layer.

$$c = \begin{bmatrix} c_{1,1} & \cdots & c_{1,n} \\ \vdots & \ddots & \vdots \\ c_{m,1} & \cdots & c_{m,n} \end{bmatrix} \tag{28}$$

After the max pooling process in (28), the feature map c becomes (29)

$$\widehat{c} = \max(c) \tag{29}$$

In this classifier,7 number of filters with a kernel size of 2 are considered. RELU activation function is used and the learning rate is 0.010.

8.5. Evaluation metrics

The three important metrics to assess the performance of classifier are precision, accuracy and F score [28].

8.6. Precision

It calculates the percentage of attacks that were correctly foreseen to all the attacked samples.

$$\text{Precision, P} = \frac{True\ positive(TP)}{True\ positive(TP) + False\ positive(FP)}$$

8.7. Accuracy

It is the ratio of instances that were accurately classified to an all instances.

$$\text{Accuracy} = \frac{number\ of\ correct\ predicted\ data}{number\ of\ testing\ data}$$

8.8. F score

It is a statistical technique for assessing a system's accuracy that considers both the precision and recall of the system.

$$F = \frac{2\ PR}{P + R}$$

Where R represents recall and p represents precision.

R can be calculated as,

$$R = \frac{True\ positive(TP)}{True\ positive(TP) + False\ Negative(FN)}$$

Table 3
Performance metrics of different classifiers.

Response	Accuracy				precision				F score			
	KNN	RF	SVM	CNN	KNN	RF	SVM	CNN	KNN	RF	SVM	CNN
Normal	70.89	91.26	89.11	96.33	89.64	89.63	92.94	93.06	72.31	88.79	81.46	95.46
Physical disturbance	75.26	93.88	85.02	96.96	83.28	85.97	89.66	92.74	73.98	85.32	83.59	95.12
Cyber disturbance	73.29	93.47	87.68	97.88	88.74	91.23.	95.93	94.68	71.22	83.36	93.62	96.95

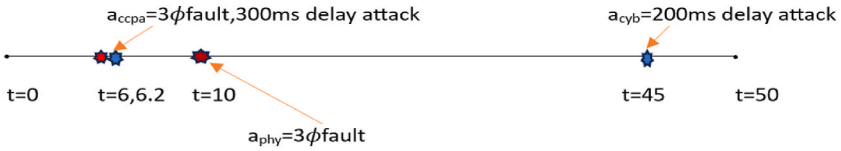


Fig. 8. Different contingency applied to time domain simulation of WSCC system.

Algorithm for selecting the effective attack detection method from a variety of classifiers:
Input: The trained dataset(A_1) and tested dataset(A_2) with label $Y_j \in ¥ = \{0,1\}$
Output: For attack detection, the best classifier $q^* \in Q$
Initialize f_1=0;
for $i \in Q$ do
train the classifier j using trained dataset A_1;
test the classifier using tested dataset A_2;
calculate f_1 score f_{1j};
if f_{1j}>f_1 then
f_1=f_{1j};
q*=j;
end if
end for
return q*;

9. Results and discussion

9.1. Detection

Among 4500 PMU measurement data, 4000 data are used to train and 500 data are used for testing the classifier. Data samples collected during each attack response are less compare to normal response. This causes imbalanced dataset, therefore by changing the decimation in "To workspace" block of Simulink model the balanced dataset can be obtained. For data pre-processing, normalisation and standardisation are not needed because the trained data samples are in per unit values which lies between 0 and 1. Consider the data set Q where it each data consist of PMU measurement represented as q_j^i for m number of instances, $i = \{1,2,3\ldots m\}$.Depending on buffer length and sampling rate of PMU, each time series length $q_j^i, j = \{1,2,3\ldots n\}$ that corresponds to time stamps $\{1,2,3\ldots t\}$.

For a set of PMU measurements Q, data sets are classified into p different classes namely,

$C_1 = \{Q_{C_1}^1, Q_{C_1}^2, Q_{C_1}^3 \ldots . Q_{C_1}^{p1}\}, C_2 = \{Q_{C_2}^1, Q_{C_2}^2, Q_{C_2}^3 \ldots . Q_{C_2}^{p2}\}, C_3 = \{Q_{C_3}^1, Q_{C_3}^2, Q_{C_3}^3 \ldots . Q_{C_3}^{p3}\}$. The three classes namely normal, physical disturbance and cyber disturbance respectively correlate to various events.

From Table 3, the results obtained indicate that the aforementioned strategies appear promising for detecting time delay attack and three phase faults. Based on the type of dataset, extracted features, and network design, different algorithms have different detection accuracy. Simulations are done on MATLAB 2021 in Intel Core i5-1135G7 CPU, 16 GB RAM DELL laptop. The analysis shown above demonstrates that CNN accurately studies PMU data to find instances of disturbance resulting from malicious measurements. Based on the analyzed performance metrics, it is concluded that CNN classifier outperforms other ML techniques. Due to the fact that the ML-based technique relies mostly on feature engineering to extract relevant information. The deep structure of the DL-based approach (CNN) allows them to automatically learn complicated features from the raw data without the need for feature engineering. Moreover, the raw datasets will be processed using DL methods to identify and extract relevant patterns. Because of its intricate structure and expertise in processing massive datasets, CNN is effective in identifying the attack.

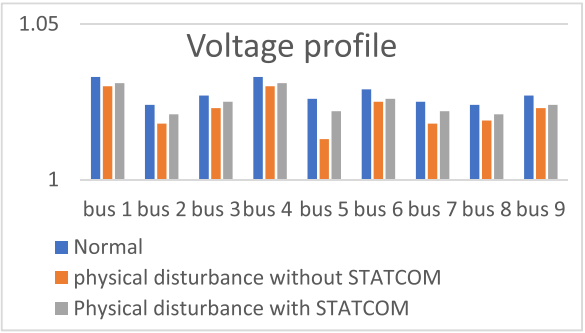


Fig. 9. Voltage profile of WSCC system.

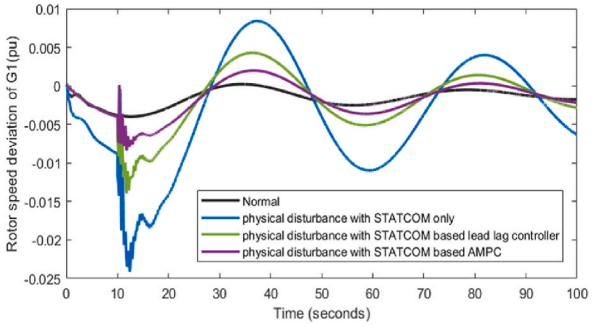


Fig. 10. Rotor speed deviation of G1.

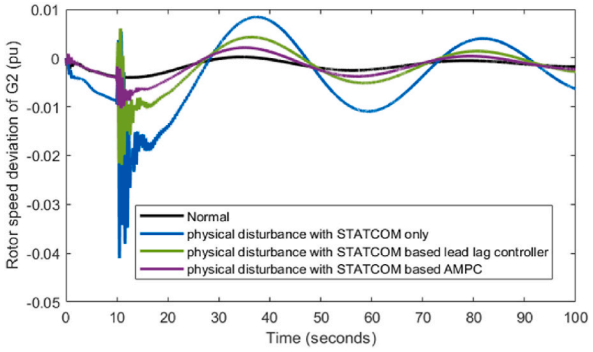


Fig. 11. Rotor speed deviation of G2.

9.2. Mitigation

Different attack scenarios are considered where the attackers target the measurement signal of STATCOM based supplementary damping controller. Fig. 8 represents different disturbance magnitude applied to time domain simulation.

Scenario 1. Physical disturbance

In the WSCC system, LLLG fault is applied as physical disturbance in the time interval between 10 and 10.1 s in the transmission line near bus 7 and simulation results are shown below. The physical disturbance vector a_{phy} is given in (30),

$$a_{phy} = \begin{cases} 0 & 0 \geq \triangle_t \leq 9 \\ 3\varphi fault & 10 \geq \triangle_t \leq 10.1 \\ 0 & 10.2 \geq \triangle_t \end{cases} \tag{30}$$

From Fig. 9, it is clear that STATCOM improve the voltage magnitude after occurrence of the three phase fault by injecting reactive power.

In all the three Figs. 10–12 the overshoot of oscillation is high in all the generators without damping controller. Therefore, after

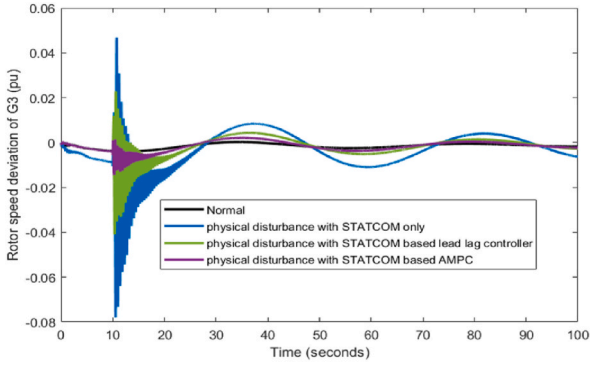


Fig. 12. Rotor speed deviation of G3.

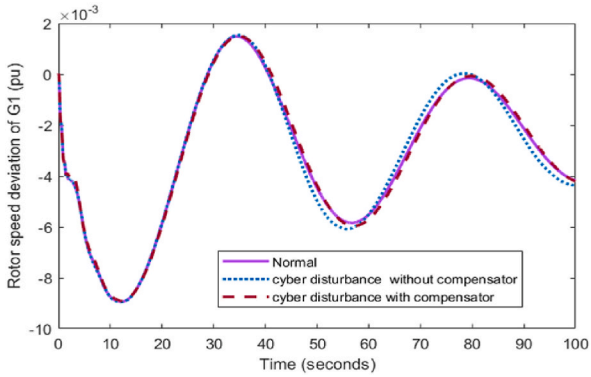


Fig. 13. Rotor speed deviation of G1.

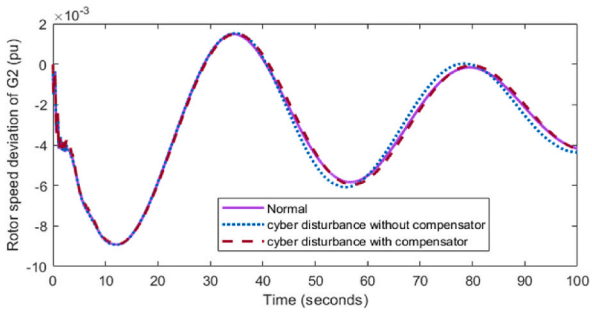


Fig. 14. Rotor speed deviation of G2.

implementation of damping controller the overshoot and settling time of oscillation is reduced. The damping of inter area oscillation using STATCOM based AMPC damping controller with RPME is better than conventional lead-lag damping controller due to online parameter identification of system.

Scenario 2. Cyber disturbance

Time delay of 150 ms is injected as cyber disturbance of t = 45th sec at the communication signal of damping controller. The cyber disturbance vector a_{cyb} is given in (31)

$$a_{cyb} = \begin{cases} 0 & 0 \geq \triangle_t \leq 44 \\ 150ms & 45 \geq \triangle_t \end{cases} \tag{31}$$

In Figs. 13–15 the solid line represents without delay attack, dashed line represents cyber disturbance with time delay compensator and Dotted lines represent cyber disturbance without compensator. The rotor speed deviation response corresponding to cyber disturbance for all the generators are shown. The simulation graph describes that the time delay compensator plays an important role

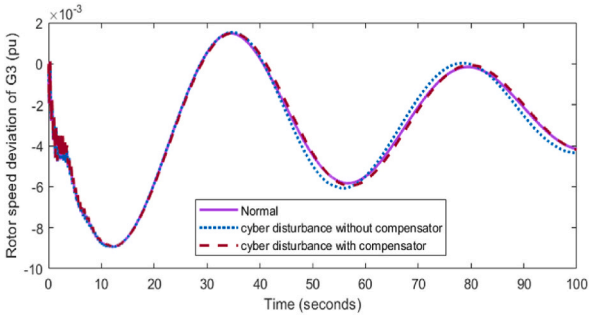


Fig. 15. Rotor speed deviation of G3.

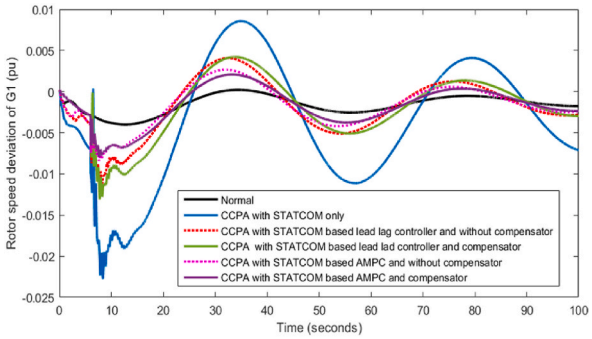


Fig. 16. Rotor speed deviation of G1.

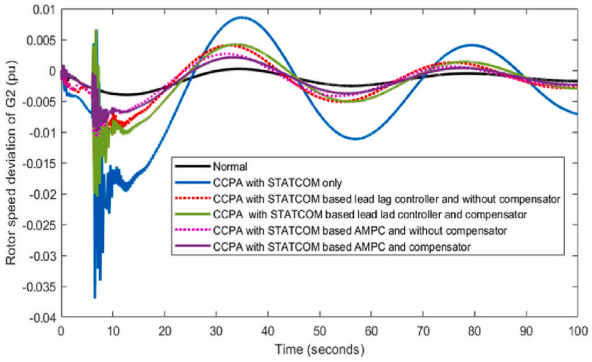


Fig. 17. Rotor speed deviation of G2.

in mitigating time delay caused by adversary.

Scenario 3. Coordinated Cyber Physical Attack

Three phase to ground fault is applied at t = 6sec to t = 6.1sec near bus 7 and a time delay attack of 200 ms is injected at the communication signal of the damping controller at t = 6.2sec. The conventional controller is an offline controller which requires retuning when operating condition changes and also has a slow response compared to the adaptive controller in reducing the oscillation. This is overcome by the implementation of an Adaptive MPC with online estimator (RPME) which is efficient in fast response. The designed RPME is efficient in detecting the change in system parameters with the least estimation error of 0.00358(shown in Fig. 20) and also updates the parameters online for the AMPC damping controller. Therefore, in Figs. 16–18 implementation of an adaptive damping controller along with a time delay compensator enhances overall stability by reducing the sudden increase in oscillation due to physical disturbance and mitigating time delay attack simultaneously in CPPS. In Fig. 19 the oscillation overshoot is reduced below 0.001 at t = 9th sec for AMPC whereas for the lead-lag controller, it is achieved at t = 11th sec. The settling time of inter-area oscillation is less in the AMPC damping controller than compared to the offline tuned damping controller.

The coordinated cyber-physical attack vector a_{ccpa} is given in (32),

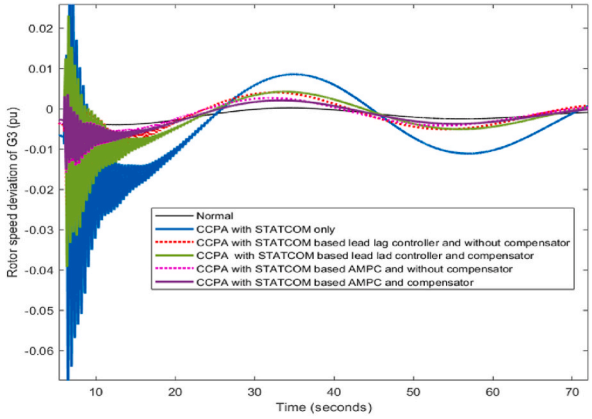


Fig. 18. Rotor speed deviation of G3.

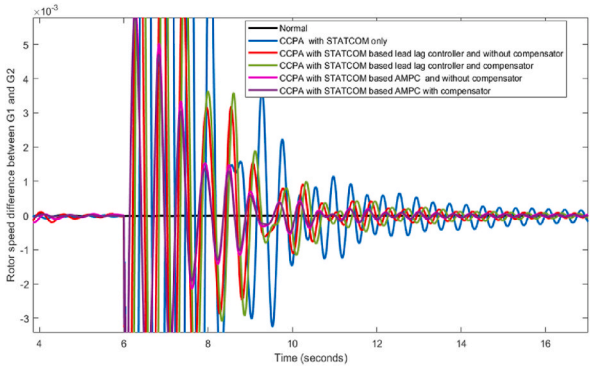


Fig. 19. Rotor speed difference between G1 and G2.

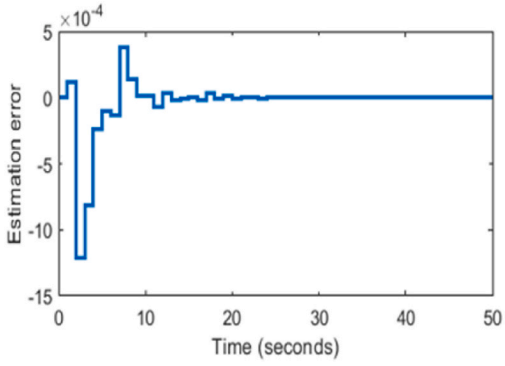


Fig. 20. Estimation error of RPME.

$$a_{ccpa} = \begin{cases} 0 & 0 \geq \triangle_t \leq 5 \\ 3\varphi fault & 6 \geq \triangle_t \leq 6.1 \\ 200ms\ delay & 6.2 \geq \triangle_t \end{cases} \tag{32}$$

Signal energy distribution across a range of frequencies can be shown using frequency domain analysis. A modified periodogram is created for each segment of the data using Welch's approach, which divides the data into overlapping segments. The power spectral density is then calculated by averaging the periodogram. The approach is based on the idea of using periodogram spectrum estimates, which result from transforming time-domain signals into frequency-domain signals.

The average power ($\mathcal{P}$) of S periodic signal is shown in (33) and (34),

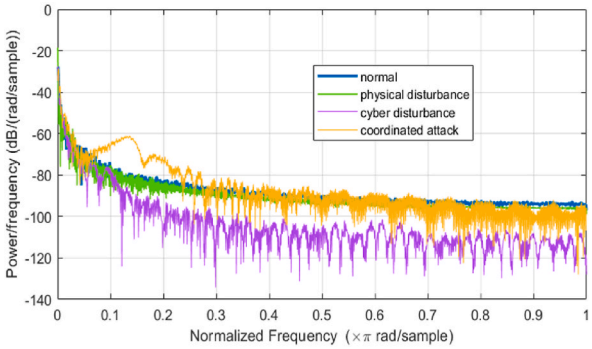


Fig. 21. Normal and attacked response using welch method.

$$P = \frac{1}{S}\sum_{n=0}^{S-1} |x(n)|^2 \tag{33}$$

$$P = \frac{1}{\omega}\int_{-\omega\backslash 2}^{\omega/2} I(\omega)\, d\omega \tag{34}$$

Where $I(\omega) = \frac{1}{S}\left|\sum_{n=0}^{S-1} x(n)e^{-j\omega nt}\right|^2$.

The aforementioned equation represents the sum of powers in distinct frequency components. The frequency domain response for normal, physical disturbance, cyber disturbance and coordinated attack is shown in Fig. 21. During normal condition of system, the power per frequency is −90 dB/rad/sample whereas for physical disturbance it is −92 dB/rad/sample. For cyber disturbance it falls below −100 dB/rad/sample. For coordinated attack response the power per frequency varies from −60 to −85 dB/rad/sample at 0.13 to 0.3 normalized frequency.

10. Conclusion

Simulation result infers that the cyber disturbance impacts the entire smart grid by causing the denial of service due to time delay injected by cyber attacker. When there is a delay in receiving the control signal to STATCOM, the resulting compensated signal also get delayed from STATCOM device, thus leading to increase in rotor speed deviation and sabotage the dynamic performance of CPPS. The proposed AMPC damping controller plays a significant role in smart grid applications. When compared to the case with conventional damping controller, the developed STATCOM based Adaptive model predictive controller with online estimator (RPME) performs better in reducing the overshoot and settling time by achieving the set point very quickly. Therefore, to dampen inter-area mode of oscillations during physical disturbance, the suggested STATCOM based AMPC controller with RPME is effective than conventional controller. In our research work, implementation of RPME will detect the change in dynamic behaviour of system due to disturbance as well as estimate the parameters in online for AMPC damping controller. This dual purpose of RPME will reduce the implementation cost too. The designed time delay compensator performs better in cyber disturbance mitigation and also improves the stability of the power system by compensating the time delays induced by the adversary. Our future work will focus on analysis and mitigation of physical and cyber disturbance in a large-scale system.

Data availability Statement

The data that support the findings of this study are available on request from the corresponding author(gysreevarshini90@gmail.com).

CRediT authorship contribution statement

G.Y. Sree Varshini: Investigation. **S. Latha:** Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

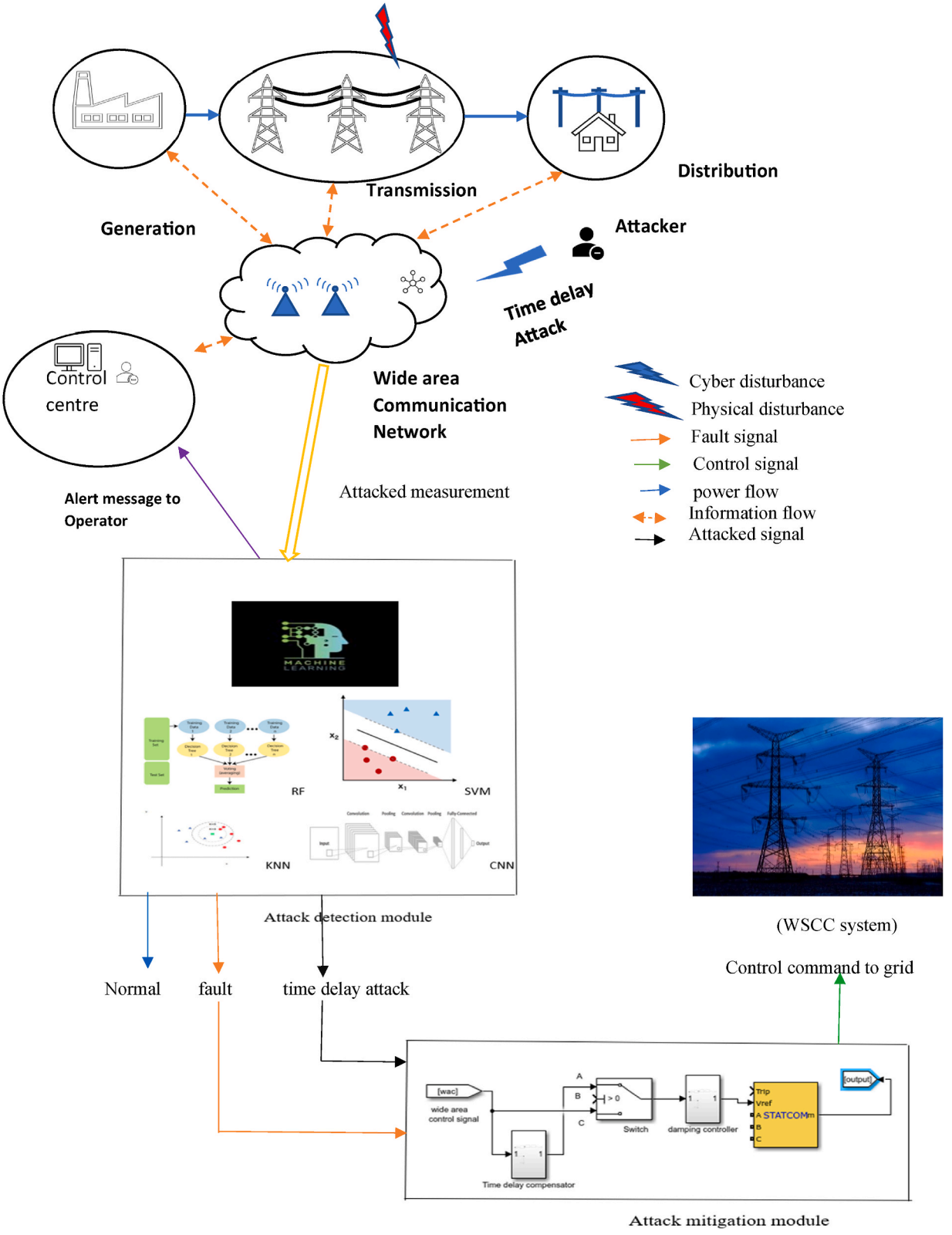


Fig. 22. An illustration of coordinated attack detection and mitigation.

References

[1] P. Kundur, Power System Stability and Control, Mc- Graw Hill, New York, 1994.
[2] Rajaa Vikhram Yohanandhan, Rajvikram Madurai Elavarasan, Premkumar Manoharan, Lucian Mihet-Popa, Cyber-physical Power System (Cpps): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications, IEEE Access, 2020, pp. 151019–151064.
[3] Alvin Huseinović, Saša Mrdović, Kemal Bicakci, Suleyman Uludag, A Survey of Denial-Of-Service Attacks and Solutions in the Smart Grid, IEEE Access, 2020, pp. 177447–177470.
[4] Mohammad Kamrul Hasan, A.K.M. Ahasan Habib, Shayla Islam, Nurhizam Safie, Siti Norul Huda Sheikh Abdullah, Bishwajeet Pandey,DDoS: distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments, Energy Rep. 9 (Supplement 10) (2023) 1318–1326.
[5] M. Govindarasu Ashok, J. Wang, Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid, Proc. IEEE 105 (7) (2017) 1389–1407.
[6] P.K. Jena, S. Ghosh, E. Koley, A binary-optimization-based coordinated cyber-physical attack for disrupting electricity market operation, IEEE Syst. J. 15 (2) (2021) 2619–2629.
[7] J. Yang, G. Sun, J. Yin, Coordinated Cyber-Physical Attack Considering False Overload of Lines, Prot Control Mod Power Syst, 2022.
[8] W. Kang, Q. Liu, P. Zhu, et al., Coordinated Cyber-Physical Attacks Based on Different Attack Strategies for Cascading Failure Analysis in Smart Grids, Wireless Netw, 2021.
[9] J. Tian, B. Wang, T. Li, F. Shang, K. Cao, Coordinated cyber-physical attacks considering DoS attacks in power systems, Int. J. Robust Nonlinear Control (2019) 1–14.
[10] Arman Sargolzaei, K.K. Yen, Mohamed Abdelghani, Time-delay switch attack on load frequency control in smart grid, Advances in Communication Technology (2013) 55–64.
[11] X. Huang, Z. Qin, H. Liu, A survey on power grid cyber security: from component-wise vulnerability assessment to system-wide impact analysis, IEEE Access 6 (2018) 69023–69035.
[12] B. Chen, S. Mashayekh, K.L. Butler-Purry, D. Kundur, Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices, IEEE Power & Energy Society General Meeting, 2013, pp. 1–5.
[13] Aaron St Leger, John James, Cyber-physical Systems Approach for Wide Area Control Applications, IEEE Texas power and energy conference (TPEC), 2018, pp. 1–6.
[14] Siddharth Sridhar, G. Manimaran, Data Integrity Attack and its Impacts on Voltage Control Loop in Power Grid, 2011 IEEE power and energy society general meeting, 2011, pp. 1–6.
[15] B. Chen, K.L. Butler-Purry, S. Nuthalapati, D. Kundur, Network Delay Caused by Cyber Attacks on SVC and its Impact on Transient Stability of Smart Grids, 2014 IEEE PES General Meeting | Conference & Exposition, 2014, pp. 1–5.
[16] Narayan Bhusal, Mukesh Gautam, Raj Mani Shukla, Mohammed Benidris, Shamik Sengupta, Coordinated data falsification attack detection in the domain of distributed generation using deep learning, Int. J. Electr. Power Energy Syst. 134 (2022).
[17] Huihui He, Shengjun Huang, Yajie Liu, Tao Zhang, A tri-level optimization model for power grid defense with the consideration of post-allocated DGs against coordinated cyber-physical attacks, Int. J. Electr. Power Energy Syst. 130 (2021).
[18] Debottam Mukherjee, Samrat Chakraborty, Y. Almoataz, Abdelaziz, Adel El-Shahat, Deep learning-based identification of false data injection attacks on modern smart grids, Energy Rep. 8 (2022). Supplement 15.
[19] K. -D. Lu and Z. -G. Wu, "Resilient event-triggered load frequency control for cyber-physical power systems under DoS attacks," in IEEE Trans. Power Syst., doi: 10.1109/TPWRS.2022.3229667..
[20] Hana Hmad Saleh, Evaluation performance of packet communication using entities, in: 2017 International Conference on Green Energy Conversion Systems, GECS), 2017, pp. 1–4.
[21] Mathworks Simevents, Users Guide, The mathworks,inc, 2015.
[22] N.G. Hingorani, L. Gyugyi, Understanding FACTS, IEEE Press, New York, 2000.
[23] W. Yao, C. Yan, X. Liu, Chuan-Ke Zhang, L. Jiang, J. Wen, Coordinated design of delay-dependent wide-area damping controllers considering multiple time delays, IET Gener. Transm. Distrib. 15 (2021) 1996–2007.
[24] Feifei Bai, Lin Zhu, Yilu Liu, Xiaoru Wang, Kai Sun, Yiwei Ma, Mahendra Patel, Evangelos Farantatos, Navin Bhatt, Design and Implementation of a Measurement Based Adaptive Wide Area Damping Controller Considering Time Delays, Electric Power System Research, 2016.
[25] B.M.R. Amin, S. Taghizadeh, M.S. Rahman, M.J. Hossain, V. Varadharajan, Z. Chen, Cyber-attacks in Smart Grid – Dynamic Impacts, Analyses and Recommendations, IET Cyber-Physical Systems: Theory & Applications, 2020, pp. 321–329.
[26] Mengze Zhou, Yuhui Wang, Anurag Srivastava, Yinghui Wu, Banerjee, Ensemble-Based Algorithm for Synchro Phasor Data Anomaly Detection, IEEE Transactions on Smart Grid, 2018.
[27] M. Esmalifalak, Nam Tuan Nguyen, R. Zheng, Z. Han, Detecting stealthy false data injection using machine learning in smart grid, IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA (2013) 808–813.
[28] D.H. Lakshminarayana, J. Philips, N. Tabrizi, A survey of intrusion detection techniques, 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), Boca Raton, FL, USA (2019) 1122–1129.
[29] Mingxiao Ma, Abdelkader Lahmadi, Isabelle Chrisment, Detecting a Stealthy Attack in Distributed Control for Microgrids Using Machine Learning Algorithms, 3rd IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), June 2020.
[30] Wenchao Li, Ping Yi, Yue Wu, Li Pan, Jianhua Li, A new intrusion detection system based on KNN classification algorithm in wireless sensor network, Journal of Electrical and Computer Engineering 2014 (2014), https://doi.org/10.1155/2014/240217. Article ID 240217, 8 pages.
[31] J. Zhang, M. Zulkernine, A. Haque, Random-forests-based network intrusion detection systems, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 38 (5) (2008) 649–659.
[32] Nabila Farnaaz, M.A. Jabbar, Random Forest Modeling for Network Intrusion Detection System, ume 89, Procedia Computer Science, 2016, pp. 213–217.
[33] Sagnik Basumallik, Rui Ma, Sara Eftekharnejad, Packet-data anomaly detection in PMU-based state estimator using convolutional neural network, Int. J. Electr. Power Energy Syst. 107 (2019) 690–702.
[34] C. Yin, Y. Zhu, J. Fei, X. He, A deep learning approach for intrusion detection using recurrent neural networks, IEEE Access 5 (2017) 21954–21961.
[35] N. Shone, T.N. Ngoc, V.D. Phai, Q. Shi, A deep learning approach to network intrusion detection, IEEE Transactions on Emerging Topics in Computational Intelligence 2 (1) (2018) 41–50.
[36] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (2015) 436–444.
[37] Jürgen Schmidhuber, Deep learning in neural networks: an overview, Neural Network. (2015) 85–117. ISSN 0893-6080.