Article:

Qiu, D., Zhang, R., Zhou, Z. et al. (2 more authors) (2023) Virtual-physical power flow method for cyber-physical power system contingency and vulnerability assessment. IET Smart Grid. ISSN 2515-2947

https://doi.org/10.1049/stg2.12143

Received: 28 April 2023 | Revised: 3 October 2023 | Accepted: 29 October 2023

IET Smart Grid

DOI: 10.1049/stg2.12143

ORIGINAL RESEARCH

Virtual-physical power flow method for cyber-physical power system contingency and vulnerability assessment

Dongmeng Qiu[1] | Rui Zhang[2] | Zhuoran Zhou[1] | Jinning Zhang[3] | Xin Zhang[1]

[1]Department of Automatic Control and Systems Engineering, University of Sheffield, Sheffield, South Yorkshire, UK

[2]National Grid ESO, Wokingham, UK

[3]School of Engineering, University of Leicester, Leicester, UK

Correspondence

Xin Zhang, Amy Johnson Building, Portobello Street, University of Sheffield, Sheffield S1 4DW, UK.
Email: xin.zhang1@sheffield.ac.uk

Funding information

UK Research and Innovation, Grant/Award Number: MR/W011360/2

Abstract

Traditional power systems have evolved into cyber-physical power systems (CPPS) with the integration of information and communication technologies. CPPS can be considered as a typical hierarchical control system that can be divided into two parts: the power grid and the communication network. CPPS will face new vulnerabilities which can have network contingencies and cascading consequences. To address this challenge, a virtual-physical power flow (VPPF) method is proposed for the vulnerability assessment of CPPS. The proposed method contains dual power flows, one is to simulate a virtual power flow from decision-making units, and the other is to simulate a physical power flow. In addition, a novel hierarchical control model is proposed that includes four layers of CPPS: the physical layer, the secondary device layer, the regional control layer, and the national control layer. The model is based on IEEE test cases using data and structures provided by MATPOWER. Denial-of-service (DoS) and false data injection (FDI) are simulated as two major cyber-attacks in CPPS. A novel vulnerability index is proposed that consists of system voltage, network latency, and node betweenness as three key indicators. This is a comprehensive and adaptive index because it encompasses both cyber and physical system characteristics and can be applied to several types of cyber-attacks. The results of the vulnerability assessment are compared in national and regional control structures of CPPS to evaluate the vulnerability of cyber-physical nodes.

KEYWORDS

cyber-physical systems, power grid, power system cyber-security and privacy, power system security

1 | BACKGROUND AND MOTIVATION

Renewable energy sources (RES) such as solar power, wind power, and hydropower have become increasingly important in recent years due to global warming mitigation and the shortage of fossil fuels. Many countries have already begun to reform their traditional energy structures. For example, China added almost 117 GW of renewable power in 2020. Wind power accounted for an important portion of total electricity generation in many countries by 2020, including Denmark (over 58%), Uruguay (40.4%), Ireland (38%), and the United Kingdom (35.5%) [1]. Europe installed 17 GW of new wind energy capacity in 2021. The European Union 27 possessed 11 GW of new wind farms [2]. This will continue to increase the share of wind power in total electricity generation. RES integrated power systems require a large number of sensors and actuators to monitor and control as a smart grid.

Therefore, a more secure information and communication systems are needed to guarantee the cyber security of the modern power system. The inclusion of modern information and communication technologies and intelligent decision-making units can be seen as an example of cyber-physical systems (CPS). The concept of CPS was first introduced by the American National Science Foundation (NSF) in 2008 [3]. Based on their definition, CPS consists of physical, biological, and manufactured systems whose operations are synthetic, monitored, and controlled by a computational system. The different parts of the physical system are connected through a network system. The CPS consists of a computational control system, a communication network, and a physical environment, forming a complex system involving real-time sensing, dynamic control and information decision-making [4]. The CPPS is an extension of the CPS in the field of power systems. In order to ensure the secure and economic operation of the power system, advanced information communication and computing technologies are increasingly deployed to realize the collection, transmission and processing of massive data with the deep integration of information decision process. CPPS, also known as "smart grid", is the future direction of power system development when there are more RES integrated to the power grid [5].

Compared with the traditional power system, CPPS will inevitably generate many new vulnerabilities across the cyber layer, making it possible to be attacked from the cyber perspective such as the Internet and digital devices. For example, on 23 December 2015, hackers attacked Ukraine's power grid. This attack resulted in the breakdown of control systems that were used to coordinate remote electrical substations [6]. In 2019, a series of severe blackouts happened in Venezuela; the country suffered unstable power supply for at least 10 days during the month of March [7].

In CPPS, a large number of intelligent sensing, measurement, and control devices generate significant amount of data. In addition, the scope of information and communication networks is expanding [8]. Problems such as data delay, packet loss, blocking, and tampering attacks that may occur in the information and communication network, which will affect the power system control centre's monitoring quality and decision-making process on the current state of the power network. As a result, the integrated CPPS will increase the system vulnerability and make it more difficult for the control centre to prevent and restore the cascading failures. In September 2003, a blackout occurred in Italy caused by the disconnection of power stations from the power grid, which resulted in the failure of several communication nodes. Eventually, the control centre could not monitor the power grid properly, leading to the disconnection of a large number of power nodes [9].

To sum up, the new cyber-physical contingencies with cyber-attacks will be introduced due to the integration of the cyber and physical networks of the power grid. New cyber-physical system vulnerability assessments are urgently required to analyse the impacts of cyber-attacks.

2 | LITERATURE REVIEW

CPPS modelling approaches are surveyed into two categories: complex network theory and cyber and power flow calculation.

2.1 | Complex network theory

The fundamental concept of complex network theory is to simplify natural complex systems by representing them as networks composed of nodes and edges. This theory is mainly used to study the influence of topology on the system with applications for CPPS network topology.

In a study conducted in 2013 [10], the connectivity of CPPS structures was represented using an adjacency matrix. Moreover, it provided a concept of “Betweenness Centrality”. This was a measure used in network analysis to quantify the importance of a node within a communication network. It was based on the number of shortest paths that pass through a particular node, indicating the extent to which that node serves as a bridge or connector between other nodes within the network. Another paper [11] incorporated betweenness centrality as a factor for vulnerability assessment. A higher betweenness centrality for a node indicated that it has a more significant role in facilitating communication or the flow of information within the network. However, a notable limitation of this article was the omission of the latency metric, which might play a crucial role in data transmission within communication systems. Considering different loading conditions, another study [12] introduced the “Vulnerability-weighted Node Degree (VWND)” index. This index indicated the importance of a node in relation to its incident edges' vulnerability.

Two stochastic models based on complex network theory were presented in papers [9, 13]. The former model presented normal distribution probability density function curves for power flow in different lines, while the latter model proposed random cyber-attacks under centralised and decentralised multi-agent control modes. Small-worldness was first defined by Watt and Strogatz [14], which was a network topology property characterised by short average path lengths between nodes and high clustering coefficients. In paper [15], a dynamic small-worldness index was proposed to assess the robustness of the CPPS. This index was used to evaluate the robustness of a realistic 1326-bus transmission network. Because the distributed structure of small-world networks made it difficult for an attacker to destroy the entire system by targeting a single node or connection, it could improve the system's resilience and adaptability to external disturbances. Particularly, the application of small-worldness index was able to better quantify the robustness of small-world networks.

In the paper [16], each power node was equipped with a cyber node to enable the controllability of power nodes as well as the observability of power transmission lines. However, the implementation of such cyber-power nodes was challenging as the topology of cyber networks and power systems were typically different. In practice, power nodes often had basic monitoring units, with information transmitted to neighbouring cyber nodes for centralised processing. The work [17] proposed a graph computing-based solution to the real-time network topology analysis for a power system. Moreover, the paper [18] provided several graph databases to simulate CPPS including Giraph, GraphLab, and GraphChi. Graph databases could effectively model the complex relationships and interdependencies between various components in a CPPS, such as elements of the power grid, communication networks, and control systems. Paper [19] presented the Gauss method and certain steps of the Newton-Raphson method which could be applied naturally to graph processing in power systems.

2.2 | Cyber and power flow calculation

Power flow calculation is a standard method for steady-state analysis of power systems. It calculates the steady-state operating state of a complex power system under normal and fault conditions [20]. The purpose of the calculation is to find out the overload and overvoltage components, optimise the power distribution and minimise power losses. The power flow calculation can adequately represent the change in the steady-state characteristics of the power system according to the topology, generation, and load variations, which is essentially based on Kirchhoff's voltage and current laws [21]. Some structures in the communication network are similar to those in the power system, for example, there is a directed current in the power system which consists of power nodes and lines, while there is a directed information flow in the communication network with consists of data nodes and links. By simplifying the features of the communication network, the information system can be simulated with the power system using the traditional power flow calculation. The obtained results can be used to analyse the node congestion and the flow of data streams. This approach which is called cyber and power flow calculation is applicable to CPPS with the relative cyber network structures.

In the paper [22], the CPPS network topology was presented in terms of a sparse matrix. The information flow in the communication system could be treated as the same pattern as the power flow in the power system. Conversion between the two flows was available via data process branch. As a result, two systems conducted co-simulation in one environment with cyber-contingency assessments. Paper [23] developed a model using a dynamic routing algorithm [24] to describe the information packet transmission in the cyber network, and simultaneously applied the dynamic load flow model to describe the power grid. Research [25] provided an optimised load-shedding policy to simulate the power-loss failures, out-of-control failures, and data-blocking (POD) failures in the process of cascade events. The research of ref. [22] provided a concept of 'Cyber Ground'. The concept enabled all the redundant nodes in the network layer being able to integrate into a cyber ground node through a data-pool branch. The advantage of this approach was that by integrating the redundant nodes, the computational pressure on the system was reduced and the computational efficiency was improved.

2.3 | Contribution

To summarise, the contributions of this research are listed as follows:

1. A virtual-physical power flow model is created based on graph theory. The model has four layers, physical layer, secondary device layer, regional control centre layer, and national control centre layer.
2. A star-structured cyber network that uses the topology of the power grid as the reference for the latency is created as the cyber layer in the CPPS.
3. A novel vulnerability index that includes system voltage, network latency and node betweenness is proposed in the paper. This is a more comprehensive assessment index, as it contains parameters for evaluating physical and cyber networks, with various types of cyber attacks in CPPS, and includes performance indicators for each cyber-physical node.

The remainder of this paper is organised as follows: Section 3 introduces the cyber contingency modelling, the virtual-physical power flow method as well as the novel vulnerability index. Section 4 includes the IEEE models for the case study. Section 5 provides the results of the simulation and vulnerability index, while Section 6 concludes the paper.

3 | CYBER CONTINGENCY MODELLING

In this section, a preliminary introduction of the two types of cyber-attacks implemented in this study is provided, followed by the introduction of the virtual-physical power flow method employed for simulation. A novel vulnerability index is developed to evaluate the cyber-attack impacts with the proposed virtual-physical power flow method.

3.1 | Cyber contingencies classification

To test the vulnerability in CPPS, cyber contingencies can be categorised into four types [22].

1) Data Error:
Data error represents FDI into the system, which is simulated as artificial value addition or reduction of the original data.

$$X_{N_E} = X_N + E_N \tag{1}$$

where

X_{N_E} : New data in node N after error data injection

X_N : Normal data in node N before error data injection

E_N : Error data injected to node N

2) Data Delay:
Data delay represents a latency which adds a time constant to the original transmission time as follows:

$$D_{N_E} = D_N + D_E \tag{2}$$

where

$$D_{N_E}\text{ : Delayed latency at node N}$$

$$D_N\text{ : Normal latency at node N}$$

$$D_E\text{: Increased latency}$$

3) Data termination loss:
Data termination means the data package is terminated or lost. Assuming the contingency occurs from t_0, the data package can be modified as follows:

$$Pack_N = \begin{cases} \{X_N, D_N\}, t < t_0 \\ \varnothing, t \geq t_0 \end{cases} \tag{3}$$

where

$$Pack_N\text{ : Data package at node N}$$

$$\varnothing\text{ : Empty set}$$

4) Data malposition:

$$Pack_N = \{X_{N+n}, ,D_{N+n}\} \tag{4}$$

where
n is an integer representing another node.
In these four cyber contingencies, the first three occur most often. Data error is modelled in FDI attacks, while data termination loss is modelled in DoS attacks, hence, the first and third cases are chosen for cyber-attacks simulation in this paper.

3.1.1 | Constrained FDI modelling

Data error can be caused by human or environmental factors. It can be called a FDI attack when the contingency is human-caused [26].

In a standard AC power system, the active power flow under non-linear expression is defined by

$$P_i = V_i^2 g_{ij} - V_i V_j g_{ij} \cos \Delta\theta_{ij} - V_i V_j b_{ij} \sin \Delta\theta_{ij} \tag{5}$$

and reactive power flow by

$$\begin{aligned} Q_i = -V_i^2 b_{ij} + V_i V_j g_{ij} \cos \Delta\theta_{ij} \\ -V_i V_j b_{ij} \sin \Delta\theta_{ij} \end{aligned} \tag{6}$$

where $i,j = 1, 2,\ldots,N$ which stands for the node index. Voltage V and phase angle θ are the system states, while active power P and reactive power Q are the parameters measured in each physical node. g_{ij} and b_{ij} denote to the conductance and susceptance between node i and j respectively [27]. In the paper [28], Gu et al. constructed an attack of the system by adjusting the state variables. Notably, when the manipulated state variable reached 90% of its original size, their proposed method identified most of the attack instances with less undetected cases. Furthermore, if the adjusted state variable was close to 95% of its original value, more FDI attack instances escaped from detection. This observation was because 95% of the manipulations were closer to the original value than 90% of the manipulations, thus resulting in an undetectable impact on the observed metrics. Therefore, in this study, the constrained FDI model also follows the rules to keep the FDI adjustment in the range of 5%–10%. Certain nodes exhibit greater underlying active and reactive power and therefore they exhibit greater magnitudes that can be manipulated and vice versa.

Should the injected data exceed a given threshold, the execution of the Optimal Power Flow (OPF) within the control centre may become unfeasible. The System Operator (SO), leveraging sophisticated algorithms, is promptly alerted of any abnormalities or contingencies within the system. Meanwhile, cyber attackers, exploiting advanced strategies, could design their attacks such that they disrupt the system to a certain extent whilst evading immediate detection by the SO [29, 30]. This paper revises the threshold in consideration to the equality and inequality constraints of power systems. If the manipulated data doesn't breach these thermal constraints, implying the control centre's ability to perform an OPF calculation, then the situation is classified as a constrained FDI attack. These observations are essential for power system state estimation that is related to the nature of stealth attacks.

A criticality-based perturbation model is used as the FDI attack model in this paper [31]. The main tampered data $s_t' = [P, Q]$ of the proposed FDI model need to satisfy physical equality and inequality constraints of power systems as following:

$$\left\| s_t' - s_t \right\|_1 \tag{7}$$

$$s.t. \quad f_{FDI}(s_t') = f'_{FDI} \tag{7a}$$

$$f_{gs}(s_t') = 0 \tag{7b}$$

$$f_{hs}(s_t') \leq 0 \tag{7c}$$

where f'_{FDI} represents the output manipulated by the attacker; $f_{gs}(\cdot)$ includes AC power flow Equations (5) and (6). Moreover, $f_{hs}(\cdot)$ consists of physical capacity limits, such as line thermal limits (8), (9), generation active power flow limits (10), and bus voltage limits (11).

$$p_{ij}^{min} \leq p_{ij} \leq p_{ij}^{max} \tag{8}$$

$$q_{ij}^{min} \leq q_{ij} \leq q_{ij}^{max} \tag{9}$$

$$P_i^{Gmin} \leq P_i \leq P_i^{Gmax} \tag{10}$$

$$v_i^{min} \le v_i \le v_i^{max} \tag{11}$$

In such an attack, when the data of FDI meet the above requirements, the attacker can utilise the data typically tolerated by OPF calculation to further increase the impact of FDI attacks without being detected [32]. In the power grid, the load capacity in every node has its limitations. P, Q limitation of node N follows $[X_{minN}, X_{maxN}]$,$X = P$,Q which is calculated based on Equation (7).

The constrained false data P_{fN},Q_{fN} are in Gaussain distribution [33] as follows:

$$P_{fN}, Q_{fN} \sim N\left(\mu, \sigma^2\right) \tag{12}$$

$$\mu = \frac{X_{minN} + X_{maxN}}{2} \tag{13}$$

$$\sigma = \frac{X_{maxN} - X_{minN}}{6} \tag{14}$$

The constrained false data by Gaussian distribution can ensure that 99.73% of the FDI attacks are within the range where the OPF can be executed, making it difficult for the SO to detect the cyber-attacks, so that the attack model is constructed to be more realistic.

3.1.2 | Denial of service modelling

Denial of service (DoS) attacks refer to an attacker who is able to interrupt the normal operation of the power grid by interfering with communication channels and attacking network protocols. Such DoS attacks can cause communication link failures and message delays, resulting in the failure to transfer information between sensors, actuators, and control systems in a timely manner. In severe cases the DoS attacks could break down the entire power systems [34, 35].

There are three types of DoS attack: Random DoS [36], Periodic DoS and Non-periodic DoS. In this paper, only Non-periodic DoS is under consideration.

In order to define the DoS attack, the structure of the information package is shown below:

$$Pack_N = \{P_N, Q_N, v_N, Z_{N1}, Z_{N2}, \ldots, D_N\} \tag{15}$$

where

N: Node index
$Pack_N$: Information package in node N
P_N: Active power of node N
Q_N: Reactive power of node N
v_N: Voltage of node N
Z_N: Impedance of a line connected to node N
D_N: Latency in node N

The equation of the DoS attack in node N in time k is presented in Equation (16):

$$Pack_N = \varnothing, \quad \text{when } t = k \tag{16}$$

When a DoS attack is launched, the control centre cannot obtain the data of all nodes in a timely manner. To deal with the DoS attack, the control centre keeps the system in operation through resilience control [37, 38]. The system operator can use the most recent transmitted data for power flow calculation for the data nodes that have been attacked by DoS. The mechanism of resilience control is presented in Equation (17), when a node is subject to a DoS attack in time k, the data collected by the control centre is represented by the following equation:

$$PF = \begin{cases} Data_N(t), \text{when node N is normal} \\ Data_N(t-k), \text{when node N is in DoS} \end{cases} \tag{17}$$

In this paper, the simulation of a DoS attack is performed in a dynamic system, where the active and reactive power of node N are set to satisfy the uniform distribution.

$$P_N, Q_N \sim U(0.95, 1.05) \tag{18}$$

where in Equation (18), P_N,Q_N are in form of per unit values.

3.2 | Virtual-physical power flow method

The basic structure of the CPPS is proposed in Figure 1. This CPPS structure represents a hierarchical control model with four layers including the physical layer, secondary device layer, regional control centre and national control centre. National and regional control modes are defined which represent two different communication network structures in CPPS. Particularly, national control mode means that the information detected in the physical layer is collected in the regional control centre and then transmitted to the national control centre for processing. Decisions made by the national control centre are then sent via the same information route to the regional control centre as well as physical layer. However, regional

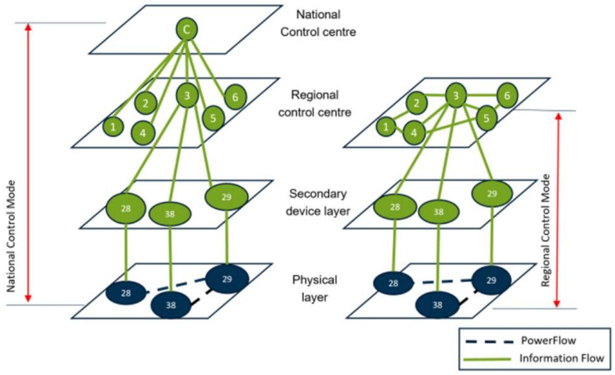

FIGURE 1 Structure of the CPPS model with national and regional control mode.

control mode represents a different communication network structure, that the information is processed and exchanged within the regional control centres of CPPS.

This paper proposes a Virtual-Physical Power Flow method (VPPF) to simulate the CPPS operation in both cyber and physical layers as shown in Figure 2. The mechanism of the model uses MATPOWER 7.1 Toolbox in MATLAB to calculate power flow in two stages within one loop of simulation. The VPPF method is integrated with the CPPS structure. During the first stage of 'Physical Power Flow', the secondary devices generate digital signals which carry the physical parameters, such as the voltage and the active and reactive power of nodes in the power grid. Then, the physical system's information is transformed into information flow in the secondary device layer.

After the secondary device layer of each node changes the physical status into information packages, the data is sent to each regional control centre. After that, every regional control centre collects all information in its area and sends it to the top layer of CPPS, which is the control centre. The control centre then uses this information to perform an OPF.

The OPF operated in the national control centre is so-called 'Virtual Power Flow'. The outcome of the OPF contains information orders to dispatch the generators. The orders are then sent from the top control centre to the regional control centres. Eventually, the orders are sent to the physical layer, where generators are deployed to change the power outputs, including active and reactive power. During the second stage of VPPF, the power grid runs another 'Physical Power Flow' using the new generation data. If the 'Physical Power Flow' in the physical layer is not within the threshold of the 'Virtual Power Flow' as that in the control centre, such virtual-physical power flow discrepancy proves that cyber contingency may occur during the information flow period. This cyber-physical discrepancy will be reflected in either the power flow in the lines or the voltage at the nodes.

In this paper, system voltage variation is chosen as one of the criteria to quantify the impact of cyber contingency on the CPPS. The procedure of the whole VPPF method is represented in the flow chart, as shown in Figure 2.

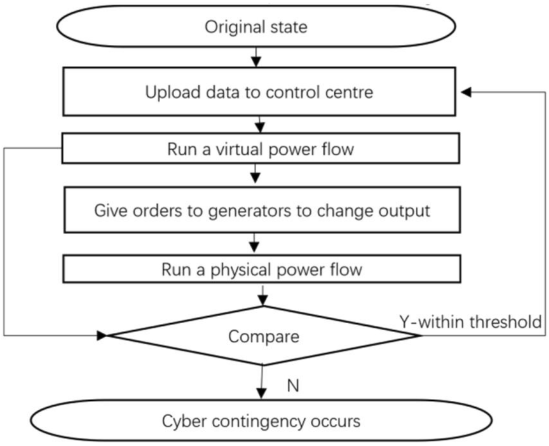
Original state
Upload data to control centre
Run a virtual power flow
Give orders to generators to change output
Run a physical power flow
Compare
Y-within threshold
N
Cyber contingency occurs

FIGURE 2 VPPF method procedure.

3.3 | Defining vulnerability index

There are several indexes for evaluating vulnerability in CPPS, considering the loss of load and robustness [44–46]. The majority of grid models employed in the current vulnerability indexes do not incorporate RES, which is required for the development and implementation of RES in the future energy landscape. Moreover, these existing indexes do not have latency indicator which would significantly improve their evaluative capabilities on cyber layers of CPPS. In this paper, both these factors are concurrently considered. The communication network is segmented, and two operational modes of national and regional control are integrated into the new vulnerability index by considering two different communication network structures in CPPS. The advantage of this approach is the scalability of the index, allowing for the future integration of new models of cyber-attack, thus enhancing its predictive and preventative capacity for potential threats in power system operation.

In order to assess and give an outcome for the vulnerability of the CPPS due to a cyber contingency, a vulnerability index is developed, which is calculated as follows:

$$I(N) = [L_R(N) + L_N(N)] \times \Delta v(N) \times C_B(N) \tag{19}$$

where in Equation (19), $L_R(N)$ is the re-routed network latency with DoS attack of node N. $L_N(N)$ is the normal network latency without DoS attack of the node N. $C_B(N)$ represents the betweenness of the node N, that is, the number of shortest paths that include the node N. Betweenness varies when the system topology is different. In this paper, both cyber network betweenness and physical network betweenness are considered. $\Delta v(N)$ represents the system voltage variation of node N when a contingency has occurred in node N.

Calculation of $\Delta v(N)$ is as follows:

$$\Delta v(N) = \sum_{i=1}^{N_{max}} |V_F(i) - V_N(i)| \tag{20}$$

where V_F represents fault voltage, and V_N represents normal voltage. In this paper, the occurrence of V_F is caused by two factors. One is an FDI attack that happens in node N. The other is a DoS attack that happens in node N. The mechanism of two types of attack is explained in Section 2.1. For each test case of data error for one node, by summing the voltage results on every bus, the total system voltage variation for the data error of the node can be obtained.

Calculation of betweenness $C_B(N)$ is as follows:

$$C_B(N) = \sum_{s \neq N \neq t} \frac{\delta_{st}(N)}{\delta_{st}} \tag{21}$$

where $C_B(N)$ represents the value of the betweenness of node N. $\delta_{st}(N)$ denotes the number of shortest paths from node s to node t via node N. δ_{st} denotes the number of all shortest paths between node s and node t.

4 | CASE STUDY

In this section, the power system model is initially presented, followed by an introduction of the communication system model. The integration methodology is employed between the two systems in CPPS model construction.

4.1 | Power system model

The IEEE-39 test case which is well known as 10-machine New-England power system, and IEEE-118 test case test case which represents a simple approximation of the American electric power system, are selected as the power grid model in this paper. The detailed data can be found in the MATPOWER 7.1 toolbox in MATLAB. To enable regional control mode as well as information flow across the zones, in the IEEE-39 test case, the power grid is divided into 6 communication zones while there are 12 zones in the IEEE-118 test case.

In order to simulate the RES penetration and their impacts on the cyber-physical power systems, within the IEEE-39 test case, each zone is integrated with certain number of 2 MW wind turbines. The total wind generation capacity is 3000 MW. A number of 1500 wind turbines are integrated to 17 nodes. Each wind turbine's power output follows a Weibull distribution [39], characterised by a scale parameter of 11.1 and a shape parameter of 2.2, simulating the hourly power output across a 24-h cycle. By modulating the quantity of wind turbines, wind power generation is manipulated to comprise approximately 50% of the overall system's power generation. For the IEEE-118 test case, the number of wind power turbines reaches 2500. A total of 5000 MW wind generation capacity is designed to ensure a comparable contribution of wind power, which accounts for approximately 50% of the total power generation within the system.

4.2 | Communication system model

The communication systems associated with the IEEE-39 test case and IEEE-118 test case have four layers. The bottom layer, called the secondary device layer, has sensors to detect data from the power network and transform it from physical value to digital signal. Accordingly, each node within the power system is outfitted with a secondary side device. Nonetheless, the configuration of the communication network is built by using star-structure of a scale-free network with each node directly connected to the regional control centre of the respective zone. The line parameter in the information network is defined as 'Latency'. Given that each device within the zone varies in its distance from the regional control centre, the calculation of latency utilises the power system as a reference, and the power system's topology is employed as a roadmap for determining the shortest path. The assumed latency of a typical line is 100 ms and the latency in a typical node is 200 ms. Dijkstra's algorithm is employed to identify the shortest path between nodes, and the calculation defines the latency for each secondary device to its directly connected regional control centre. This method can also be utilised to calculate the latency from the regional control centres to the national control centre.

All 39 buses in the power system are divided into six zones, while in the IEEE-118 test case, there are 12 zones created. Each zone has its regional control centre, which should be powered by the power network. Therefore, the control centres are assumed to be located in certain nodes in the power grid. For each zone, the location of regional control centres is determined where the average transit time from other nodes in the zone is minimal. As a result, Dijkstra's algorithm is utilised to locate the node with the shortest average transit time to other nodes within each zone, utilising the power system topology as a reference.

The zones and the regional control centres' locations of the IEEE-39 test case are shown as green colour nodes in Figure 3. The nodes with wind power turbines are shown in this figure as well. The IEEE-39 test case adopts the communication networks structure in regional control mode, which means the regional control centres will communicate between each communication zone. Zone latency is calculated as the average latencies of all nodes to their regional control centre within each communication zone. An example of

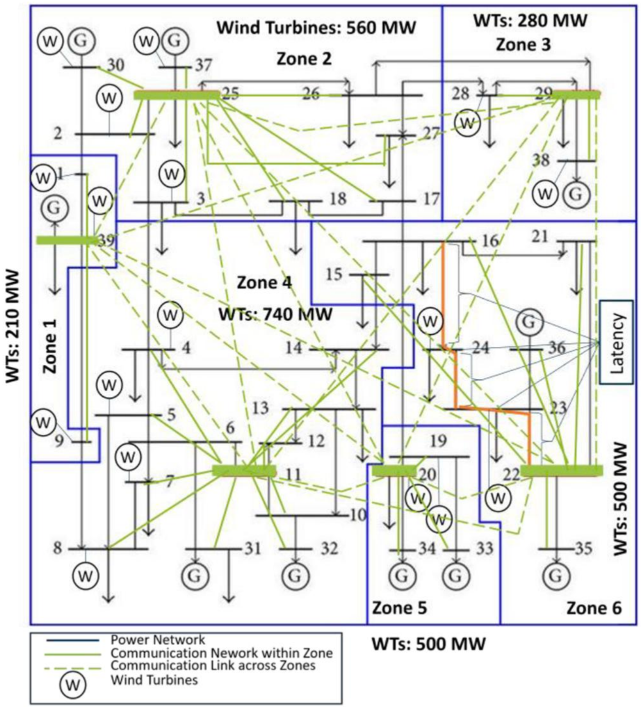

FIGURE 3 IEEE-39 test case of CPPS with communication networks in regional control mode.

latency calculation for each information route is presented with orange line, which represents the latency from node 16 to regional control centre node 22. The average latency within each communication zone in IEEE-39 test case is shown in Table 1. Node 39, 25, 29, 11, 20 and 22 are assumed to be the regional control centres in IEEE-39 test case. The latency results show that the larger zone such as zone 4 has higher zone latency.

The locations of regional control centres in IEEE-118 test case with the number of wind turbines in each zone are shown in Figure 4. Table 2 shows the latency from regional control centres to national control centre. Node 69 is determined to be the national control centre in IEEE-118 test case by Dijkstra's algorithm.

4.3 | CPPS model construction

A graph-based model of CPPS is constructed in this paper. The model combines a physical power system with a communication network to accomplish cross-domain simulation. A logical adjacency matrix M_P is produced for the graph-based power grid. Because the physical layer and the secondary device layer have the same topology structure, in the matrix, these two layers are represented by the same variable M_P. M_C stands for the control centre layer in the communication system and M_{ZC} represents zone control centre layer. Each layer is composed of a logical adjacency matrix as follows:

TABLE 1 Regional control centres location for IEEE-39 system.

Zone name	Regional control centre	Average zone latency (ms) in each communication zone
1	Node 39	300
2	Node 25	550
3	Node 29	300
4	Node 11	650
5	Node 20	400
6	Node 22	500

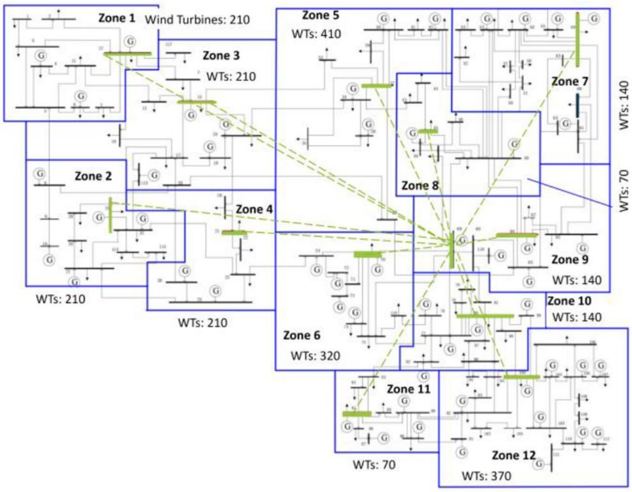

FIGURE 4 IEEE-118 test case of CPPS with communication network zones in national control mode.

$$M_\omega = \begin{bmatrix} M_{1,1} & \cdots & M_{1,n} \\ \vdots & \ddots & \vdots \\ M_{m,1} & \cdots & M_{m,n} \end{bmatrix} \tag{22}$$

where

$$M_{m,n} = 0(\text{no direct link}), 1(\text{link exists})$$

$$\omega : \text{Type of matrix}(\text{P}, \text{C}, \text{ZC}, \text{etc.})$$

Next, the whole CPPS network is the combination of adjacency matrixes of the four layers. Combining different layers will create four new sub-matrices describing the cross-domain links between layers, M_{PZC}, M_{ZCP}, M_{ZCC}, and M_{CZC} represent links between physical layer to zone control centre, zone control centre to control centre according to the definition of relevant sub-matrices, as shown below in Equation (22).

$$M_{CPPS} = \begin{bmatrix} M_P & M_{ZCP} & 0 \\ M_{PZC} & M_{ZC} & M_{ZCC} \\ 0 & M_{CZC} & M_C \end{bmatrix} \tag{23}$$

where

M_P: physical layer and secondary device layer
M_{ZC}: zone control centre layer
M_C: control centre layer
M_{PZC}: Links from physical layer to zone control centres

TABLE 2 Regional control centres location for IEEE-118 system.

Zone Name	Regional control centre	Latency to national control centre (ms)
1	Node 12	2100
2	Node 31	1500
3	Node 15	1800
4	Node 21	1500
5	Node 37	1200
6	Node 70	300
7	Node 59	900
8	Node 45	600
9	Node 66	600
10	Node 80	600
11	Node 85	1200
12	Node 100	1200

M_{ZCP}: Links from zone control centres to physical grid
M_{ZCC}: Links from zone control centres to control centre
M_{CZC}: Links from control centre to zone control centres

5 | RESULTS AND DISCUSSION

CPPS simulations are conducted using MATLAB for the IEEE-39 test case and IEEE-118 test case. This section will simulate the cyber-attack models and discuss the contingency assessment outcomes of adjacency matrix, system voltage, network latency and node betweenness of CPPS. Vulnerability index is presented at the end of this section.

5.1 | Adjacency matrix

Figure 5 illustrates an IEEE-39 test case adjacency matrix with binary digits in regional control mode. In this adjacency matrix, '0' denotes no physical or cyber connection between nodes. '1' with grey colour denotes there is a physical connection between nodes. '1' with red colour denotes there is a communication link (information route) between nodes, and in this case the nodes are connected to control centres are highlighted in red colour. This adjacency matrix is generated in Equation (22).

This adjacency matrix can be used to study the routing problem of CPPS. For example, Route 1 stands for a basic information route within zone 6 of regional control mode of communication networks as shown in Figure 5. Data from node 15 are sent to its own regional control centre node 22 via information route (15, 22). After a short period of time with latency, the decision is sent back to node 15. Route 2 represents an example of a cross-region routing problem. When data need to be sent from node 3 to node 4, the information route is across two zones. Firstly, data are sent to regional control centre node 25 via the information route (3, 25) within zone 2. After that, data are sent to the regional control centre node 11 via the information route (11, 25) which is across zone 2 and 4. Then data are sent to node 4 through information route (4, 11) within zone 4, and this round-trip Route 2 is completed.

Figure 6 presents an example of information routing problem in national control mode of communication networks in IEEE-39 test case. Route 3 starts at node 3 and goes through the information route (3, 25) to node 25 of a regional control centre, then through the information route (25, 16) to the node 16 of national control centre. The information is centrally processed in node 16 of national control centre, and the generation dispatch instructions are sent back to node 3 via the same Route 3.

In the IEEE-118 test case, the adjacency matrix is of similar information routing structure and generation dispatch orders. However, the adjacency matrix consists of a 118 by 118 matrix which is too large to display in this part.

5.2 | System voltage

The system voltage variation discussed in this paper consists of two parts, one generated by the FDI attack and the other by the DoS attack. The system voltage variation is represented as a percentage to the highest variation case in order to make it compatible in vulnerability index across different size and structure of CPPS.

5.2.1 | System voltage variation made by FDI attack

In this case, the FDI attack modelling in Equation (12), is applied to each node respectively. After that, the system voltage variation in the CPPS due to FDI will be calculated in Equation (20) respectively. The system voltage variation also considers the volatility of wind power output which is modelled by Weibull distribution on a 24-h cycle. Therefore, for the FDI attack on each node, the test case simulates 24 attacks, corresponding to one attack per hour. Then, the system voltage variations which are generated by these 24 FDI attacks are summed as a final system voltage variation for this specific node over 24 h. The test case will then be continued to the

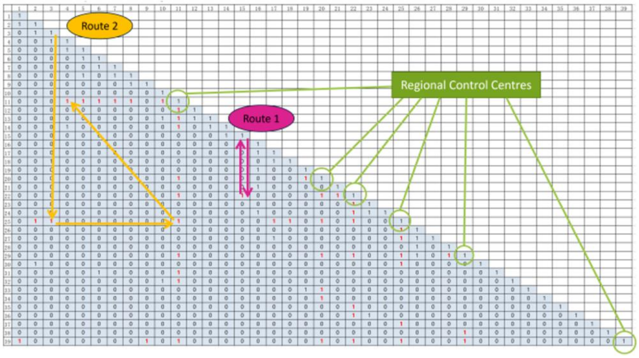

FIGURE 5 IEEE-39 test case adjacency matrix (regional control mode).

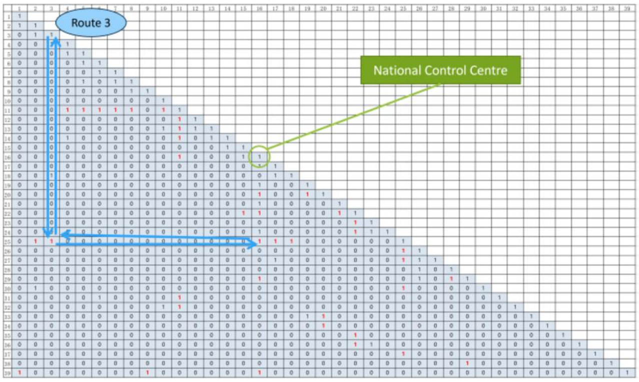

FIGURE 6 IEEE-39 test case adjacency matrix (national control mode).

next node so that the system voltage variation of all nodes can be obtained.

Figure 7 presents the results of the system voltage variation under FDI attack of each node respectively in the IEEE-39 test case. The results are arranged according to each communication network zone in order to compare the results across different zones.

In Figure 7a, system voltage variation is ranked in percentage for each bus in the IEEE-39 test case. The results are analysed against each individual node as well as for each communication network zone. For each individual node under the FDI attack, it is found that nodes 26, 4, and 8 represent the highest system voltage variation, while the nodes 3, 14, 24, and 32 show the relatively low variation in the system voltage. This is primarily due to the different locations of node which are subject to different physical properties across CPPS. For example, the nodes 26 and 4 are both located at the edge of the physical network of CPPS (as shown in Figure 3), so that the higher system voltage variations are observed due to the weaker reactive power control on the edge and remote locations of the power network. In contrast, the nodes which are located in the central parts of the power network or connected with generators will both receive stronger support in terms of voltage regulation, therefore the nodes 3, 14, 24, and 32 have the lower system voltage variations. For each different zone, the higher system voltage variations are observed in zones 2, 4, and 6 respectively, because these zones have larger physical networks in their regions but less generators to regulate the voltage. In addition, a large amount of wind power generation is integrated in these zones to make voltage regulation more challenging. For zones 1, 3, and 5, there are smaller physical power networks but relatively more generators in order to control the voltage. Therefore, the system voltage variations are minimised in these zones. Figure 7b shows the system voltage variations caused by FDI attacks in the IEEE-118 test case. The similar results are observed that system voltage variations are highly related to the physical power networks. In summary, the system voltage variation is highly dependent on the physical network topology as well as the distribution of generation. This system voltage variation index is capable of assessing the vulnerability on the physical aspects of CPPS.

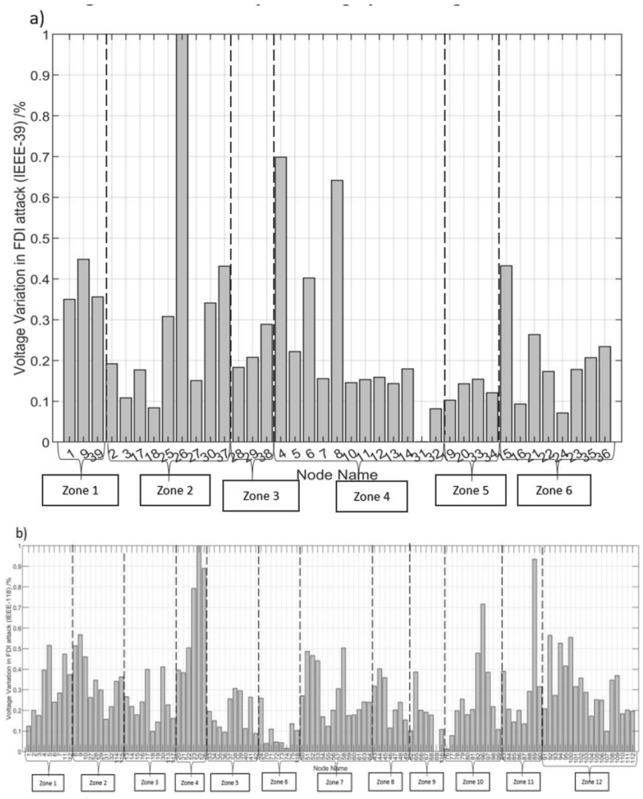

FIGURE 7 System voltage variation of (a) IEEE-39 and (b) IEEE-118 test case under FDI attacks.

A comparison of Figure 7a,b provides an understanding of how the system voltage variations behave in two CPPS with different sizes and communication structures. This is attributed to the fact that the manipulated data from the constrained FDI attack is impacted by the active and reactive power of each node, coupled with the wind power generation which introduces further volatility into the system. In the IEEE-39 system, zone 2 includes the nodes with the minimum and maximum system voltage variations respectively. On the other hand, the IEEE-118 test case with the increased number of nodes, presents a widely spread-out voltage variations across different zones. However, the system voltage variation results appear to be independent of each communication network zone in the cyber aspects of CPPS. As a result, for FDI attacks, the topology knowledge of a power network allows the attacker to analyse the best location for an FDI attack in terms of voltage variations. Therefore, the defence of FDI can focus mainly on the change in the topology, such as moving target defence [40].

5.2.2 | System voltage variation made by DoS attack

From the mechanism of DoS attack modelled in Equation (15), DoS is applied to only affect one specific communication node of CPPS. However, the system voltage variations are influenced across the whole CPPS. Figure 8, which presents the results of the system voltage variation of each DoS-attacked node in the IEEE-39 test case. The result shows the more uniformly distributed of system voltage variation across all the nodes under the DoS, with a variance of 13.4 in system voltage variation of the IEEE-39 test case. However, in FDI attack cases, the variance of system voltage variation can reach as high as 37.5, indicating the locational impact of FDI attack is much greater than the DoS attack.

By comparing Figure 8a,b, it can be seen that DoS attacks cause a different impact across different sizes of CPPS, with the variance of system voltage variations becoming more uniform in the larger-scale systems. By comparing the IEEE-39 test case and IEEE-118 test case, the variance of system voltage variations in IEEE-118 test case is greatly reduced to

0.274. This result suggests that in larger CPPS, the system voltage impacts caused by DoS attacks on individual node become similar and more uniformly distributed. When a DoS attack occurs, it is difficult to determine the exact location of such attack by the system voltage variations as an indicator, as each node has the similar influence on system voltages subject to DoS attacks. In summary, the system voltage variations become a less effective indicator to assess the DoS attack in CPPS.

5.3 | Network latency

Latency of communication networks of CPPS is investigated for DoS attack of CPPS. The initial study found that the DoS attack on individual node has minimal impacts comparing with DoS attack on the regional control centres. Therefore, the DoS attack on each regional control centre is investigated respectively.

5.3.1 | Latency in IEEE-39 test case

Figure 9 shows the network latency before and after the DoS attack for each node on the regional control centre in the CPPS. Shortest path of communication network is re-routed when the original communication link is interrupted, which is caused by a DoS attack on each regional control centre. When a regional control centre is attacked by a DoS, the communication links that between this regional control centre and connected nodes are all interrupted within this zone. As a result, the nodes in the DoS-attacked zone will re-route to a nearest neighbouring zone where another regional control centre is still in service, which results in an increased network latency of each node in the re-routed communication links. The normal network latency as well as the re-routed network latency are compared in the form of network latency. Results that in dark red represents normal network latency in each region, while bars in light red represent the re-routed network latency under DoS attack.

In the normal network latency without cyberattack, nodes 17, 18, 4, 8, 14, 15 have higher values of network latency, while nodes 39, 25, 29, 11, 20, and 22 have the lowest network latency in each zone. This is because these nodes have to pass through multiple intermediate nodes to reach the regional control centre, and the latency in the communication network is calculated on the shortest path of the physical network topology as an assumption. As a result, the shortest path in communication networks of CPPS is the key factor that influences the network latency without DoS attack.

However, after the DoS attack with the re-routed communication networks, re-routed network latency of regional control centre nodes has a significant increase comparing with the normal operating condition. This is because the regional control centres are usually directly connected with other control centres. When DoS attack occurs, the direct communication links become interrupted, so that the DoS-attacked regional control centres which are located at the centre of each zone need a longer latency to reach the neighbouring zone via the re-routed communication links. For other nodes that are located at the edge of each zone, there are two types of results: 1) nodes such as 16, 17, and 32 that are located at the edge of the zone as well as at the edge of the whole CPPS, their re-routed network latency become relatively high. 2) nodes that are located at the edge of

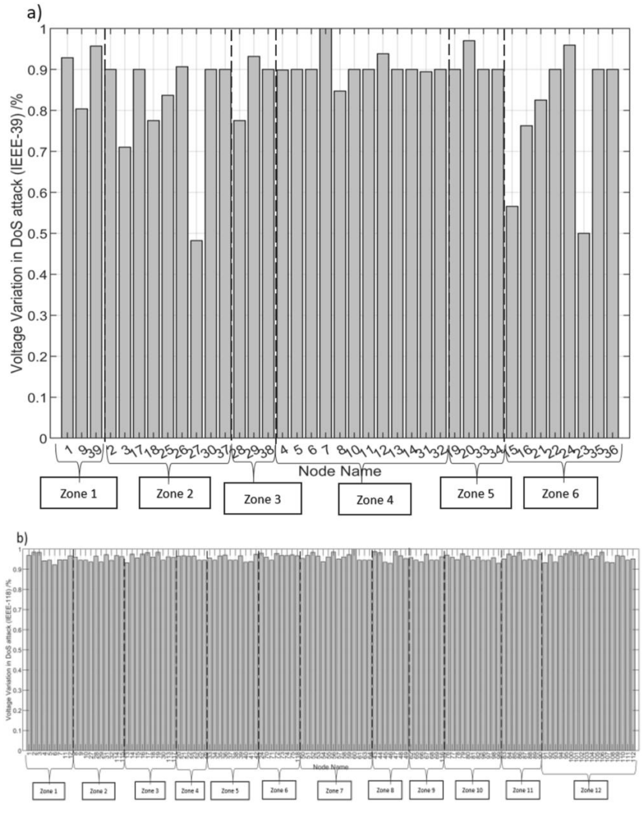

FIGURE 8 System voltage variation of (a) IEEE-39 and (b) IEEE-118 test case under DoS.

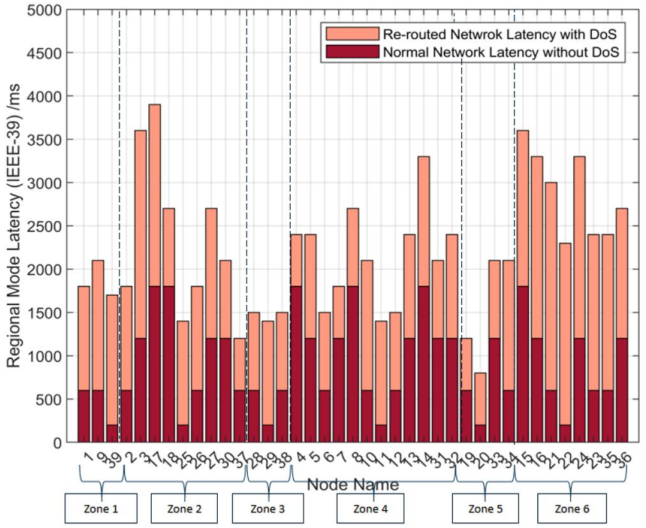

FIGURE 9 Network latency of IEEE-39 test case.

their own zone but close to the neighbouring zones, their re-routed network latency has minimal increase under DoS attacks, because their re-routed communication links are closer to the regional control centre of the nearest zone, such as nodes 4, 7, and 19. Moreover, for different zones, the more interconnected zone 4 has the relatively less network latency increase than the more isolated zone 6. This shows that the zone with more interconnected communication links become more resilient to the DoS attacks.

It is also found that FDI attack has minimal impacts on the latency of communication networks, the network latency is mainly impacted by the DoS attacks.

5.3.2 | Latency in IEEE-118 test case

Figure 10 shows the network latency of IEEE-118 test case in normal and re-routed network latency under the DoS attacks. Nodes 9, 10, and 26 have the highest values of network latency in the normal operating conditions, while nodes 12, 31, and 15 have the lowest normal network latency. These are due to the locations of the nodes with different length of communication links as shown in Figure 4. The nodes which are further away from the regional control centre have a longer network latency. These results are similar to the IEEE-39 test case.

The results also show that the larger CPPS such as IEEE-118 test case in Figure 10 has the higher average network latency of 2000 ms across all nodes, which is compared with the average network latency of 1500 ms in the IEEE-39 test case. This is due to the larger size of the CPPS with communication networks that are distributed across longer distance. However, such larger CPPS has the lower network latency increase under the DoS attacks. This is due to the more interconnected zones of IEEE-118 test case that can provide a more resilient network in response to the DoS attacks.

The results show that the network latency is a feasible indicator to identify the impacts of DoS attacks on the different nodes of CPPS with various zone size and node locations.

5.4 | Node betweenness

Node betweenness is calculated based on both power and communication networks respectively. The results demonstrate the physical (power) node as well as cyber (communication) node's centrality in a networked CPPS. The results of both physical node and cyber node's betweenness are added together to form the 'cyber-physical node betweenness' in the CPPS. The results of node betweenness are calculated in Equation (21).

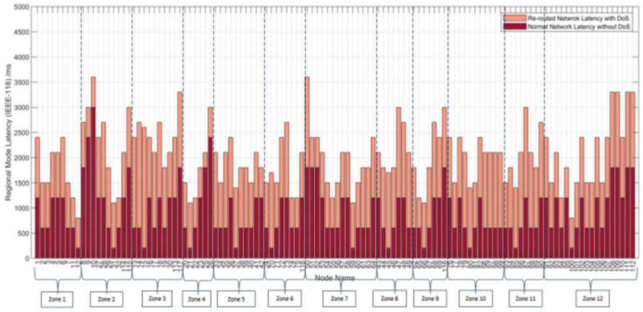

FIGURE 10 Network latency of IEEE-118 test case.

5.4.1 | Node betweenness in IEEE-39 test case

The results of the cyber-physical node betweenness in the IEEE-39 test case of CPPS is presented in Figure 11. Nodes 16, 14 and 4 have the highest values of betweenness in physical network. These are due to the power network topology. Nodes with higher betweenness in physical network demonstrates that they are more interconnected with other nodes, therefore they become one of the intermediate nodes in these shortest paths between other nodes. While nodes with less connectivity have lower values of node betweenness, because there are less number of shortest paths go through these nodes. There are some nodes which have no betweenness in the physical network, for example, nodes 30, 37 and 28. Because they are not the intermediate node of any shortest path, due to their locations which are at the edge of the physical network.

In communication network, nodes 39, 25, 29, 11, 20, and 22 have the highest value of betweenness in cyber network, as they are all regional control centres which are centralised in their own communication zones. In these regional control centres, nodes 39 and 29 have the lowest cyber network betweenness among regional control centres, because zone 1 and zone 3 only have three cyber nodes with less communication links. While node 11 owns the highest cyber network betweenness since zone 4 have the most cyber nodes and communication links in the IEEE-39 test case.

The distribution of cyber-physical node betweenness varies due to the different topology of power and communication

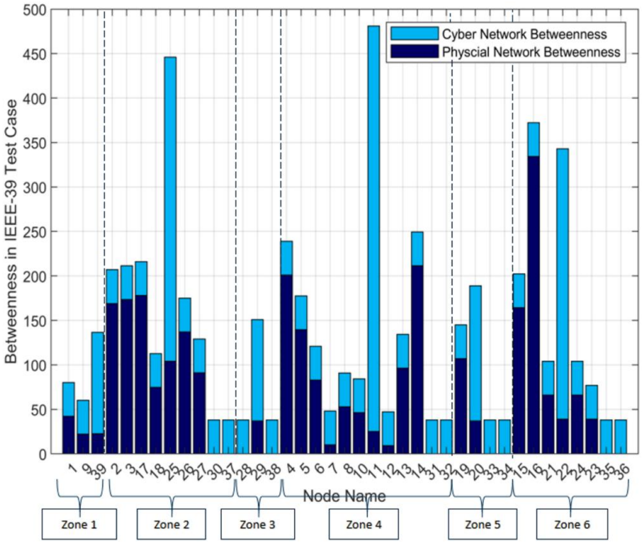

FIGURE 11 Cyber-physical node betweenness of IEEE-39 test case.

networks. The power network is a more distributed network with power flow being distributed across the whole system, while the communication network is more centralised network with information flows that require to be connected via certain nodes, such as regional control centre in each zone. For example, node 11 has a low physical network betweenness which has minimal impacts on the power network, but it has very high cyber network betweenness indicating the cyber importance of node 11 as its role of regional control centre. In contrast, node 16 has a very high physical network betweenness, as it is located in the centre of power networks, but it has very low cyber network betweenness in the communication network. The cyber-physical node betweenness is added together to better reflect the cyber-physical nodal importance of CPPS.

Therefore, the cyber-physical node betweenness can be considered as an effective indicator to assess the node importance of both cyber and physical networks.

5.4.2 | Node betweenness in IEEE-118 test case

Figure 12 represents the results of cyber-physical node betweenness in IEEE-118 test case. Similar to the results of the IEEE-39 test case, nodes 12, 31, 15, 21, 37, 70, 59, 45, 66, 80, 85, and 100 in IEEE-118 test case have higher cyber network betweenness compared to other nodes. Each of these nodes is a regional control centre in each communication zone. In the physical network, nodes with high values of physical network betweenness are not evenly distributed in each zone, for example, nodes in both zone 1 and zone 7 have relatively lower physical network betweenness due to their remote locations in power networks, while most of nodes in zone 9 and zone 10 have higher physical network betweenness due to their central locations of power networks.

By comparing Figure 11 with Figure 12, it can be seen that the range of node betweenness in the IEEE-39 test case is from 50 to 500, while in the IEEE-118 test case the range of node betweenness is from 100 to 3500. The average value of node betweenness in IEEE-118 test case is much higher than that in IEEE-39 test case. This is due to the fact that in the larger CPPS, there are more nodes and associated shortest paths in both physical and cyber networks.

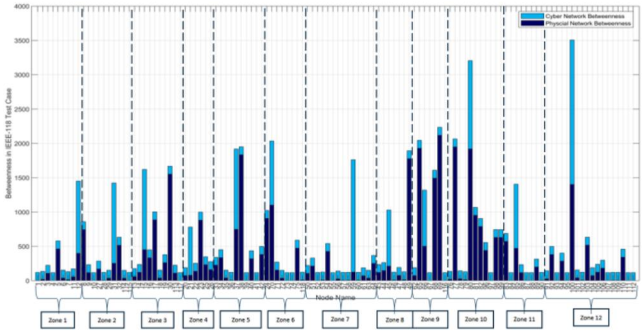

FIGURE 12 Cyber-physical node betweenness of IEEE-118 test case.

The cyber-physical node betweenness can be considered as an indicator to assess the impacts of various cyberattacks on CPPS. For example, FDI attack may become more effective on the node with higher physical network betweenness, as it is more interconnected with other power nodes that may have higher impacts on VPPF. In the cyber network, the higher the cyber network betweenness, the more likely the node will encounter cyber contingencies such as DoS attack, due to the centralised communication network structure used in these test cases. Therefore, the higher the cyber-physical node betweenness, the higher the vulnerability of the node under cyberattacks.

5.5 | Vulnerability index assessment

Figures 13 and 14 present the vulnerability index of each node in IEEE-39 test case and IEEE-118 test case respectively. The results of vulnerability index are calculated in Equation (19), which consists of three indicators: system voltage variation, network latency, and node betweenness. As shown in Figure-13, nodes 17, 4, 14, and 16 have the highest values of the vulnerability, which means they are the most vulnerable nodes

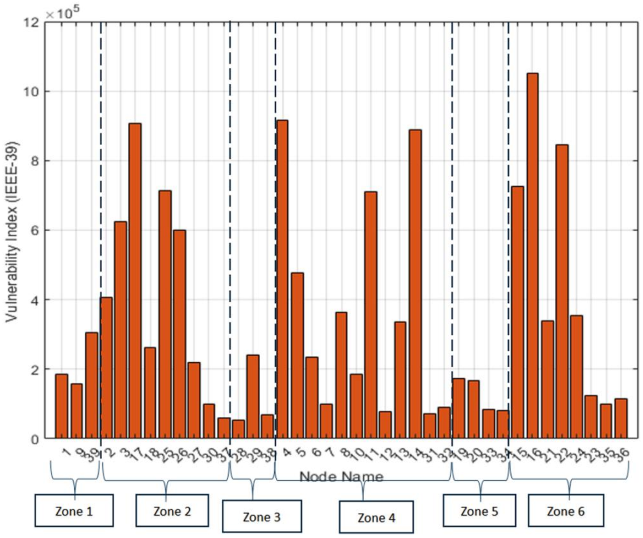

FIGURE 13 Vulnerability index in IEEE-39 test case.

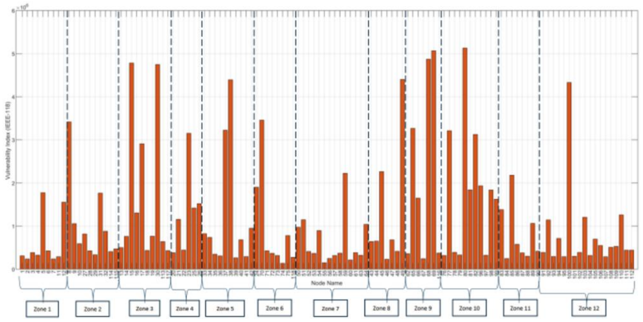

FIGURE 14 Vulnerability index in IEEE-118 test case.

of CPPS subject to cyber contingencies. This is due to the nodes 17, 14, and 16 which have very high re-routed network latency after the DoS attacks, as well as the high physical network betweenness. The high vulnerability of node 4 is due to the high voltage variation after FDI attack. The vulnerability indexes of nodes 28, 38, and 12 are relatively low, because they are all located at the edge of the networks with low level of node betweenness. Certain low vulnerability nodes are also near to a synchronous generator that are less affected by voltage variations and have lower re-routed latency of communication networks.

In Figure 14, nodes 80, 69, 68, and 100 have higher values of the vulnerability index, which means they are expected to be the most vulnerable nodes in this CPPS. Nodes 80, 68, and 100 are regional control centres, while 69 is the national control centre. This simulation results illustrate that control centres are more vulnerable than normal nodes, and they can have higher impacts on the CPPS when under a cyberattack. However, there are some exceptions such as in zone 4 where node 21 is the regional control centre, but node 23 in the same zone has a much higher vulnerability index than node 21. This is due to the higher physical network betweenness as well as higher voltage variation of node 23, so that its physical vulnerability is outweighed over the cyber vulnerability. It is found that not only the regional control centre of communication network that needs to pay attention to cybersecurity, but also the physical vulnerability of the power network needs to take into consideration, as the cyberattacks will impact the power networks such as voltage variations.

6 | CONCLUSION

This paper proposes a VPPF method to assess cyber contingencies in the CPPS. A hierarchical cyber-physical system with four layers is proposed with national and regional control structure of CPPS. In order to build communication networks for the analysis of cyber contingencies, communication zones are designed by using star-structured communication networks with various network latencies, which are developed based on the power system topology of IEEE-39 and IEEE-118 test cases. Constrained FDI attacks and DoS attacks are simulated to evaluate vulnerability of cyber and physical nodes in CPPS. The proposed novel vulnerability index includes system voltage variation, network latency, and node betweenness as the three indicators. It is found that system voltage indicator is more effective in detecting the FDI attacks, as such attacks can be identified by the impacts on the physical network including network topology and generation distribution. As for the network latency indicator, results show that the zone with interconnected communication links become more resilient to the DoS attacks. The node betweenness indicator provides an effective way to address 'cyber-physical node betweenness' in the CPPS due to the different topologies of power and communication networks. The results show that the higher the cyber-physical node betweenness, the higher the vulnerability of the node under cyberattacks.

The overall vulnerability index identifies the low vulnerability of nodes with the following three types: nodes at the edge of the networks with lower node betweenness, nodes near a synchronous generator that are less affected by voltage variations, and nodes with low re-routed latency of communication networks. The vulnerability index also identifies that control centres have the highest vulnerability, so that they are more vulnerable to cyberattacks.

AUTHOR CONTRIBUTIONS

Dongmeng Qiu: Formal analysis; methodology; software; writing – original draft; writing – review & editing. **Rui Zhang**: Investigation; resources; validation; visualisation. **Zhuoran Zhou**: Investigation; methodology; validation. **Jinning Zhang**: Methodology; resources; validation; writing – review & editing. **Xin Zhang**: Conceptualisation; funding acquisition; investigation; supervision; writing – original draft.

ACKNOWLEDGEMENTS

This work has been funded by UK Research and Innovation Future Leaders Fellowship (grant number: MR/W011360/2): 'Digitalisation of Electrical Power and Energy Systems Operation (DEEPS)'.

CONFLICT OF INTEREST STATEMENT

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

DATA AVAILABILITY STATEMENT

Data will be made available for research and non-commercial purpose, and can be requested from the corresponding author.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

ORCID

Xin Zhang https://orcid.org/0000-0002-6063-959X

REFERENCES

1. Henner, D., REN21: Renewables 2021 Global Status Report (2021). [Online]. https://abdn.pure.elsevier.com/en/en/researchoutput/ren21(5d1212f6-d863-45f7-8979-5f68a61e380e).html
2. Komusanac, I., et al.: Wind Energy in Europe 2021 (2022)
3. Gill, H.: From vision to reality: cyber-physical systems. Presentation HCSS, National Workshop on New Research Directions for High Confidence Transportation CPS: Automotive , Aviation , and Rail. 91(2), 60 (2008)
4. Wang, Y.: Modeling Technique and Vulnerability Assessment of Elecrical Cyber Physical System Considering Cyber Attacks. Zhejiang University (2019)
5. Liu, M., et al.: Enhancing Cyber-Resiliency of DER-Based SmartGrid: A Survey (2023). [Online]. Available: http://arxiv.org/abs/2305.05338
6. Kostyuk, N., Zhukov, Y.M.: Invisible digital front: can cyber attacks shape battlefield events? J. Conflict Resolut. 63(2), 317–347 (2019). https://doi.org/10.1177/0022002717737138

7. Dube, R., Castro, M.: Venezuela Blackout Plunges Millions into Darkness. The Wall Street Journal (2019). [Online]. Available: https://www.wsj.com/articles/venezuela-blackout-stretches-across-country-closing-schools-and-businesses-11552053011.2022
8. Liu, Y., et al.: Smarter grid in the 5G era: a framework integrating power Internet of things with a cyber physical system. Front. Commun. Netw. 2, 1–14 (2021). https://doi.org/10.3389/frcmn.2021.689590
9. Gao, X., et al.: A stochastic model of cascading failure dynamics in cyber-physical power systems. IEEE Syst. J. 14(3), 4626–4637 (2020). https://doi.org/10.1109/JSYST.2020.2964624
10. Sanchez, J., Caire, R., Hadjsaid, N.: ICT and Electric Power Systems Interdependencies Modeling. no. 139, pp. 7–12. ETG-Fachbericht (2013)
11. Myhre, S.F., et al.: Modeling interdependencies with complex network theory in a combined electrical power and ICT system. In: 2020 International Conference on Probabilistic Methods Applied to Power Systems, PMAPS 2020 - Proceedings (2020). https://doi.org/10.1109/PMAPS47429.2020.9183667
12. Zhu, W.: Cyber-physical System Failure Analysis Based on Complex Network Theory, pp. 6–8. July (2017)
13. Gao, X., Li, X., Yang, X.: Robustness assessment of the cyber-physical system against cascading failure in a virtual power plant based on complex network theory. Int. Trans. Electr. Energy Syst. 31(11), 1–27 (2021). https://doi.org/10.1002/2050-7038.13039
14. Watts, D.J., Strogatz, S.H.: Collective dynamics of "small-world" networks. Nature 393, 440–442 (1998) [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/9623998
15. Zhu, W., Milanović, J.V.: Assessment of the robustness of cyber-physical systems using small-worldness of weighted complex networks. Int. J. Electr. Power Energy Syst. 125(March 2020), 106486 (2021). https://doi.org/10.1016/j.ijepes.2020.106486
16. Pan, H., et al.: Modeling and vulnerability analysis of cyber-physical power systems based on community theory. IEEE Syst. J. 14(3), 3938–3948 (2020). https://doi.org/10.1109/JSYST.2020.2969023
17. Dai, J., et al.: Graph computing-based real-time network topology analysis for power system. IEEE Power Energy Soc. General Meet. (2019). https://doi.org/10.1109/PESGM40551.2019.8973614
18. Liu, X., et al.: Graph database and graph computing for cyber-physical power systems. In: 2nd IEEE Conference on Energy Internet and Energy System Integration, EI2 2018 - Proceedings. 1, 1–5 (2018). https://doi.org/10.1109/EI2.2018.8581924
19. Di, W., Qinglai, G.: Feasibility Analysis and Application of Graph Processing in Gauss and Newton-Raphson Power Flow Calculation, pp. 1–6 (2017)
20. Li, Z., et al.: Coordinated transmission and distribution AC optimal power flow. IEEE Trans. Smart Grid. 9(2), 1228–1240 (2018). https://doi.org/10.1109/TSG.2016.2582221
21. Sachdev, M.S., Ibrahim, S.A.: A modified Newton Raphson load flow technique and its use in simulating line and transformer outages. IFAC Proc. Vol. 12(5), 126–131 (1979). Part 1. https://doi.org/10.1016/S1474-6670(17)65295-9
22. Xin, S., et al.: Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. IEEE Trans. Smart Grid. 6(5), 2375–2385 (2015). https://doi.org/10.1109/TSG.2014.2387381
23. Gao, X., Peng, M., Tse, C.K.: Cascading failure analysis of cyber physical power systems considering routing strategy. IEEE Trans. Circuits Syst. II: Express Briefs 7747 (2021). https://doi.org/10.1109/TCSII.2021.3071920
24. Echenique, P., Gómez-Gardeñes, J., Moreno, Y.: Improved routing strategies for Internet traffic delivery. Phys. Rev. E. 70(5), 56105 (2004). https://doi.org/10.1103/PhysRevE.70.056105
25. Liu, H., et al.: Impact of inter-network assortativity on robustness against cascading failures in cyber–physical power systems. Reliab. Eng. Syst. Saf. 217(September 2021), 108068 (2022). https://doi.org/10.1016/j.ress.2021.108068
26. Ahmed, M., Pathan, A.S.K.: False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. Complex Adaptive Syst. Model. 8(1), 4 (2020). https://doi.org/10.1186/s40294-020-00070-w
27. Higgins, M., et al.: Topology learning aided false data injection attack without prior topology information. IEEE Power Energy Soc. General Meet. 2021, 1–5 (2020). https://doi.org/10.1109/PESGM46819.2021.9638211
28. Chaojun, G., Jirutitijaroen, P., Motani, M.: Detecting false data injection attacks in AC state estimation. IEEE Trans. Smart Grid. 6(5), 2476–2483 (2015). https://doi.org/10.1109/TSG.2015.2388545
29. Du, M., Wang, L., Zhou, Y.: High-stealth false data attacks on overloading multiple lines in power systems. IEEE Trans. Smart Grid. 14(2), 1321–1324 (2023). https://doi.org/10.1109/TSG.2022.3209524
30. Zhang, J., et al.: Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? IEEE Trans. Power Syst. 33(5), 4775–4786 (2018). https://doi.org/10.1109/TPWRS.2018.2818746
31. Zheng, Y., et al.: Vulnerability assessment of deep reinforcement learning models for power system topology optimization. IEEE Trans. Smart Grid. 12(4), 3613–3623 (2021). https://doi.org/10.1109/TSG.2021.3062700
32. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14(1), 1–33 (2011). https://doi.org/10.1145/1952982.1952995
33. Yang, T., Liu, Y., Li, W.: Attack and defence methods in cyber-physical power system. IET Energy Syst. Integr. 4(2), 159–170 (2022). https://doi.org/10.1049/esi2.12068
34. Liu, S., Liu, X.P., El Saddik, A.: Denial-of-Service (dos) attacks on load frequency control in smart grids. IEEE PES Innovative Smart Grid Technologies Conference, pp. 1–6. ISGT (2013). https://doi.org/10.1109/ISGT.2013.6497846
35. Li, X., et al.: A novel state estimation method for smart grid under consecutive denial of service attacks. IEEE Syst. J. 17(1), 513–524 (2022). https://doi.org/10.1109/JSYST.2022.3171751
36. Ding, K., et al.: DoS attacks on remote state estimation with asymmetric information. IEEE Trans. Control Netw. Syst. 6(2), 653–666 (2019). https://doi.org/10.1109/tcns.2018.2867157
37. De Persis, C., Tesi, P.: Resilient control under denial-of-service. IFAC. 19(3), 134–139 (2014). https://doi.org/10.3182/20140824-6-za-1003.02184
38. Lian, Z., et al.: Distributed resilient optimal current sharing control for an Islanded DC microgrid under DoS attacks. IEEE Trans. Smart Grid. 12(5), 4494–4505 (2021). https://doi.org/10.1109/TSG.2021.3084348
39. Arslan, T., Bulut, Y.M., Altın Yavuz, A.: Comparative study of numerical methods for determining Weibull parameters for wind energy potential. Renew. Sustain. Energy Rev. 40, 820–825 (2014). https://doi.org/10.1016/j.rser.2014.08.009
40. Liu, B., et al.: Random-enabled hidden moving target defense against false data injection alert attackers. Processes. 11(2), 348 (2023). https://doi.org/10.3390/pr11020348

How to cite this article: Qiu, D., et al.: Virtual-physical power flow method for cyber-physical power system contingency and vulnerability assessment. IET Smart Grid. 1–15 (2023). https://doi.org/10.1049/stg2.12143