IET Cyber-Physical Systems: Theory & Applications

Research Article

Cyber attacks in smart grid – dynamic impacts, analyses and recommendations

ISSN 2398-3396
Received on 17th December 2019
Revised 11th April 2020
Accepted on 28th July 2020
E-First on 2nd October 2020
doi: 10.1049/iet-cps.2019.0103
www.ietdl.org

B.M. Ruhul Amin[1] ✉, Seyedfoad Taghizadeh[1], Md. Shihanur Rahman[2], Md. Jahangir Hossain[3], Vijay Varadharajan[4], Zhiyong Chen[4]

[1]*School of Engineering, Macquarie University, Macquarie Park, NSW 2113, Australia*
[2]*Department of System Design and Engineering, Australian Energy Market Operator (AEMO), Melbourne, VIC 3000, Australia*
[3]*School of Electrical and Data Engineering, University of Technology Sydney (UTS), Sydney, NSW-2007, Australia*
[4]*Faculty of Engineering and Built Environment, The University of Newcastle, Callaghan, NSW 2308, Australia*
✉ *E-mail: aminbmruhul@gmail.com*

Abstract: Cyber attacks can cause cascading failures and blackouts in smart grids. Therefore, it is highly necessary to identify the types, impacts and solutions of cyber attacks to ensure the secure operation of power systems. As a well-known practice, steady-state analysis is commonly used to identify cyber attacks and provide effective solutions. However, it cannot fully cover non-linear behaviours and cascaded blackouts of the system caused by dynamic perturbations, as well as provide a post-disturbance operating point. This study presents a novel approach based on dynamic analysis that excludes the limitations of the steady-state analysis and can be used in the events of various cyber attacks. Four types of common attacks are reviewed, and their dynamic impacts are shown on the IEEE benchmark model of the Western System Coordinating Council system implemented in MATLAB Simulink. Then, recommendations are provided to enhance the security of the future smart power grids from the possible cyber attacks.

1 Introduction

The malicious cyber attacks are severe disruptive events which cause unsatisfactory behaviour of smart grids and lead to mal-operation of computers and electronic controls, tripping of motors and generators, load shedding and cascading failure of the system [1]. This paper discusses some major issues concerning the common security threats to the access points of digital protective relays. In a critical structure like power grid, the most common form of cyber attacks are false or spurious data injection to the computer-aided system operating devices, denial of service (DoS) events on the device to device communication facilities, malicious switching behaviour of circuit breakers (CBs)/isolators and so on.

Cyber attacks targeted to a smart grid includes password pilfering, DoS, man-in-the-middle, replay, jamming channels, popping the human–machine interface, integrity violations, privacy violations and so on. The impacts of the cyber attacks can cause variety of severe consequences in the smart grid, from energy theft to a massive blackouts or destruction to critical infrastructures such as prime movers or generators. Several high profile attacks on critical infrastructures and industrial control systems are reported in recent years [2]. Different types of DoS attacks such as jamming, spoofing and data flooding attacks can cause from delaying the time-critical messages to complete denial-of-service by making the communication with a device to be impossible or causing the device to crash or reset. The Aurora Generator Test and coordinated cyber attacks in the Ukraine power station prove the severity of disruptive switching executions and DoS attacks to the digital protection devices of power systems [3, 4].

A cyber attack can be initiated by professional hackers, malicious insiders or organised criminals. The attacker can exploit the flaws and vulnerabilities in software and communication protocols to electronically invade the power system operational networks. Attackers can gather a system's information after extensive reconnaissance of targeted networked components and utilise the weakness of physical security policies to initiate attacks on substations, control centres, transmission and distribution infrastructures by compromising critical protective devices. Protective devices (i.e. relay) in the substation not only operate during faults or abnormal situations, but also can be opened and closed remotely by the system operator via wireless communication channels. Digital protection devices, which are operated via unsecured communication networks, are vulnerable to several cyber threats [5].

Several attempts have been performed in the literature to increase the cyber-security of the power grid against possible cyber attacks using steady-state analysis. In [6–9], authors showed that false data injection (FDI) attacks can mislead the state estimation process of the power grid using topology information of an attack-free system. A comprehensive review of FDI attacks and detection techniques on compromised system topology information can be found in [10, 11]. Kim and Tong [12] proposed a heuristic method to prevent the undetectable attacks performed by the weak adversaries with only local information. In [13], a mathematical framework is proposed to quantify the economic impact of the topology data attacks in electricity market when virtual biding strategy is conducted by an attacker. This method performs the steady-state analysis on a transmission line to calculate the adversary's profit at particular virtual biding buses. In [14], a steady-state based metaheuristic optimisation algorithm is proposed to solve three attack models. However, the steady-state analysis is performed based on power-flow analysis which does not fully cover a system's non-linear behaviours and dynamic response.

For instance, the variation of frequency, which is always assumed to be constant in power-flow analysis, is not taken into account in steady-state analysis. Moreover, the steady-state analysis is unable to address the sequential switching events as well as providing a post-disturbance operating solution. In [15], a cyber-resilient line current differential relay (LCDR) is proposed which can detect FDIAs against LCDR, but is limited to FDI attacks on LCDRs only. Attack resilient distance protection scheme is proposed in [15, 16] though the cyber vulnerabilities still exist for over-current relays and directional relays. A novel risk assessment method is proposed in [17] by analysing the relationship among protective device settings, protection and CB logics during cyber attacks. Although the presented risk assessment method is applicable to identify the power grid behaviour during

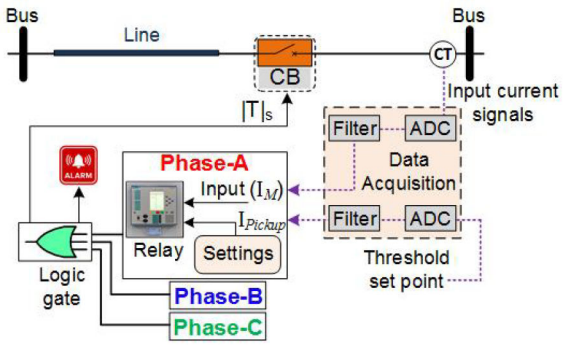

Fig. 1 *Schematic diagram of digital overcurrent relay*

cyber attacks, it is not effective during normal physical faults. The power grid behaviour during faults and cyber attacks could be significantly different and need to be considered while performing a risk assessment. To address these gaps, this paper presents the dynamic impact analyses of a real interconnected power system during different types of cyber attacks.

In [18], an attempt is conducted to investigate the impact on the cyber-physical power grid in cases where communications and operations of distributed energy resources are manipulated by an adversary. In [19], research is conducted to assess the dynamic impacts of hypothesised cyber attacks on substations and concluded that the dynamic study is more capable in detecting cascading failure due to cyber attacks. However, Ten *et al.* [19] only evaluate the dynamic impacts of one type of attack, which is the disrupt switching attack, and the dynamic impact analysis of other types are not covered. Random switching attacks, data integrity attacks, replay attacks and DoS attacks are most possible threats to generate false trip-commands to the relays [20]. Therefore in this paper, a rigorous analysis is performed to investigate the dynamic performance of an IEEE benchmark model of Western System Coordinating Council (WSCC) during the event of four types of cyber attacks in the system. Moreover, the dynamic impact of the system during attacks is compared with the system's dynamic behaviour during normal physical faults. As a result, the efforts made in this paper open a wide horizon of exploring and developing new cyber-attack detection and mitigation techniques, which utilise distinctive dynamic responses of the system properties.

The rest of the paper is organised as follows. Section 2 presents the protection setting and configuration of a digital overcurrent relay. Section 3 reviews different types of attack models. In Section 4, the description of an interconnected power system model is illustrated. Then in Section 5, the dynamic impact of attack models is depicted and critically discussed followed by the recommendations and future directions. Section 6 presents the conclusion of this research.

2 Protection settings and configurations

In this section, a set of protection configurations with inherent digital logic processing capability of a digital overcurrent relay, which is the main target of cyber attacks, is discussed. A simplified schematic diagram of the digital overcurrent relay is shown in Fig. 1. The data acquisition block performs the front-end functions of the digital protective relay. Data acquisition block is connected to a database through a communication channel to store fault information. Each set of current signals at each node is a source of continuous measurement of current obtained from the current transformer (CT), which can be obtained as follows:

$$z_{\mathrm{I}} = \left[I_{i_{\mathrm{re}}}^{a,b,c} \ldots, I_{i_{\mathrm{im}}}^{a,b,c}\right]^{\mathrm{T}} \tag{1}$$

where $I^{a,b,c}$ is the measured phase currents for ith node. In order to present an accurate model of the microprocessor based overcurrent relay, the analogue input current signals from CT are converted into digital signals by analogue-to-digital conversion (ADC). An ADC converts certain range of the input signal using a certain number of bits (N) and the minimum recognisable change of the signal can be assumed as

$$\Delta X = \frac{2X_{\max}}{2^N} \tag{2}$$

where $2X_{\max}$ is the measured phase currents and N is number of bits for the current channels. A filter is also used to extract the fundamental signal and eliminate both the aliasing frequencies and the signal spectrum that are not utilised by the overcurrent relays. The values of the processed current signals from the CT measurements are fed to the relay protection block which compares the measured values with the threshold or pickup values.

The equivalent phasor measuring unit is used for the estimation of the current's amplitude at each phase. The rated current contributed from the generator during fault can be calculated by using the following mathematical equation:

$$I_{\mathrm{Rated}} = \frac{P}{\sqrt{3} \times V_{L-L} \times \cos\theta} \tag{3}$$

where P is the power, $V_{\mathrm{L-L}}$ is the line-to-line rms voltage and $\cos\theta$ is the power factor of the generating resource.

The decision threshold or pickup value is to be set with care, i.e. taking into account the maximum expected load current and minimum fault current in the protection relay operation. The usual pickup current (I_{pickup}) of the relay generally lies in between the maximum load currents and the minimum fault currents of a system which can be written as [20]

$$I_{\mathrm{load}_{\max}} < I_{\mathrm{pickup}} \leq I_{\mathrm{fault}_{\min}} \tag{4}$$

where $I_{\mathrm{load}_{\max}}$ is the maximum load currents and $I_{\mathrm{fault}_{\min}}$ is the minimum fault currents.

The pickup current should be above the maximum load current to ensure the relay does not trip at normal load conditions, which is normally within a continuous range on relay's available settings. The relay pickup tap setting can be formulated by [21]

$$\mathrm{PS}_i = \frac{I_{\mathrm{pickup}}}{\mathrm{CTR}_i} \tag{5}$$

where I_{pickup} is the primary pickup current and CTR_i is the CT ratio.

In this paper, different levels (e.g. high, warning and normal) of the threshold values for the overcurrent relay at each phase are considered according to the information of phase current under maximum loading and short-circuit conditions to configure the activation of the relay operation. This threshold setting should also comply with practical range of the relay settings which normally ranges from 50 to 200% of the rated currents [20]. In this paper, the following expression is used to determine different levels of the current thresholds:

$$I_{\mathrm{R}} = \begin{cases} \lim\limits_{I_{\mathrm{TH}} \to \infty} I_{\mathrm{High}}, & I_{\mathrm{TH}} \leq I_{\mathrm{M}} < \infty \quad (6a) \\ \lim\limits_{I_{\mathrm{N}} \to I_{\mathrm{TH}}} I_{\mathrm{Warning}}, & I_{\mathrm{N}} \leq I_{\mathrm{M}} < I_{\mathrm{W}} \quad (6b) \\ \lim\limits_{0 \to I_{\mathrm{N}}} I_{\mathrm{Normal}}, & 0 < I_{\mathrm{M}} \leq I_{\mathrm{N}} \quad (6c) \end{cases}$$

The high range (I_{High}) is the over current range if the measured current from CT exceeds the threshold value for a given fault. The warning range (I_{Warning}) lies between the threshold and normal current limits subject to a time delay set for a very short duration of overcurrent spike to activate alarm. The third range is the normal range (I_{Normal}), which is above zero but less than the normal current limit for safe operation.

A suitable minimum grading time interval for overcurrent relay operation can be calculated as follows [21]:

$$T_{op} = \left\lceil \frac{E_{CT}}{100} \right\rceil \times t + t_{CB} + t_0 + t_s \quad (7)$$

where E_{CT} is the allowable CT ratio error (%), t is the nominal operating time of relay close to the fault location, t_{CB} is the CB interrupting time, t_0 is the protection relay overshoot time and t_s is the safety margin of relay operation. The speed of the overcurrent relay depends on the shorter data window of the current magnitude measurement as it enhances the faster relay decision-making capability.

Generally, a deterministic approach is used for decision making where the decision concerning state of the protected plant is taken by comparing measured criteria values with appropriately set thresholds. The decision-making problem is formulated as the discrimination is made when the criterion value is higher than the pre-defined current pickup value (threshold), which eventually separates two classes of events, e.g. normal operation versus fault conditions. Once the actual current value is obtained from data acquisition, this current is fed into the relay protection algorithm decision-making unit block, which compares this value with the pickup value to determine alarm or tripping logic. If the input current is within the warning range, it executes alarm signal, and if it exceeds the pickup value, the relay will generate a trip signal to open the CB. The following flag determines the signature of a fault and the relationship of the fault status, measured relay current (I_M) and threshold limit (I_{pickup}) which can be written as

$$F_s = \begin{cases} 0, & 0 < I_M \leq I_{pickup} \\ 1, & I_{pickup} < I_M < \infty \end{cases} \quad (8)$$

In this paper, the overcurrent functionality is used for each of the three phases and the output of the relay is connected to the OR logic to generate the trip signal. The OR logic enables the control signal of the relay to activate when a fault occurs on any of the three phases. The outputs of these relays are connected to the OR logic to generate the trip signal for CBs with a very little time delay to avoid unnecessary tripping. However, if the duration of shorter overcurrent period is less than the set time value, relay will raise alarm signal whereas it will issue a trip signal in case if the duration of overcurrent exceeds the delay.

In (8), when the measured CT current through the relay (I_M) flows below the threshold limit (I_{pickup}), the fault status (F_s) will be set to '0' whereas F_s will be set to '1' when I_M exceeds I_{pickup} due to a fault in the system. The relays apply the set of protection logics according to the fault status flag and if fault exists, the relays immediately issue a trip signal to corresponding CBs to isolate the fault as

$$\left|T\right|_s = \begin{cases} 1, & F_s = 0 \rightarrow \text{CB close} \\ 0, & F_s = 1 \rightarrow \text{CB open} \end{cases} \quad (9)$$

3 Attack models

According to the North American Electric Reliability Corporation (NERC)'s Protection System Misoperation Task Force reports, over 20% of the protection misoperations occur due to relay/CB malfunctions [22]. One possible reason for the protection misoperation is critically identified as malicious cyber attacks due to the compromise of security flaws and vulnerabilities in the software and information channels. Successful cyber attacks against protection systems result an unusual operation of the relays due to insufficient requirements of authentication [20]. In such a case, it is very important to understand the impacts of malicious activities on the operational behaviour of the power system.

Digital overcurrent relays are an integral part of the modern interconnected power system that are used to operate the system safely and securely during the event of credible contingencies in the power grid. Digital overcurrent relays usually protect the major components of power systems from high surge of currents, which could severely damage the components and be one of the main reasons of blackout, if not properly mitigated. When an overcurrent relay is compromised by an attacker, the power injections and load demand would largely be impacted and even disconnected from the main system. The compromised relay could change the topology of the power grid and consequently cause unstable operation of the grid. Eventually, it is also challenging to distinguish the operation of overcurrent relays for short circuit faults and cyber attacks. Therefore, digital overcurrent relay scheme is considered here as a critical component to investigate the vulnerabilities of different attack scenarios on the relay operation.

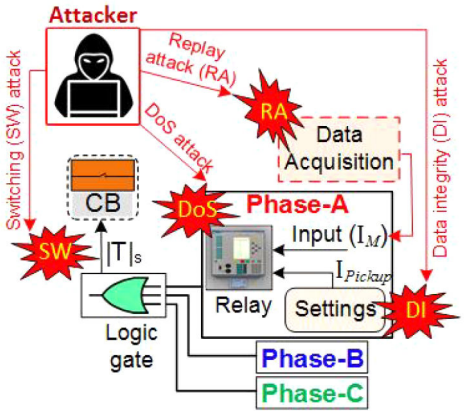

Fig. 2 *Attacks on digital overcurrent relay*

Information and communication technology based digital protection system is one of the most critical infrastructure where an attacker sends preset thresholds to a relay or directly/indirectly tampers with a relay's commands to affect the relay operation and limit its availability. The attacks on relays mainly involve: (i) compromising the relay trip signals, (ii) sending spurious commands to the relay through a compromised channel to cause an incorrect operation and (iii) manipulating the relay settings to cause unstable operation during fault events. A series of preplanned relay failures can cause power outages. In this paper, a realistic case is considered to model the cyber attacks where the adversary can have access to a subsystem and manipulate the information from a remote computer. Accordingly, four different classes of possible attack models as shown in Fig. 2 are reviewed and discussed below.

3.1 Switching attack

Attacks on the switching mechanism or relay tripping functions that change the CB's mode of operation generally stand for switching attacks. A random switching vector signal $\boldsymbol{S}(x,t)\epsilon\mathbb{R}^{m\times 1}$ is considered where $\boldsymbol{S}(x,t)$ dictates when to open or close a specific breaker for a given switching attack. The attack vector could be $\boldsymbol{S}(x,t) = [s_1 s_2 \ldots s_m]^T = [00\ldots0]^T$, where m is the number of targeted CB. A malicious switching attack, from an external adversary, can have access to the functions of a digital relay which controls the tie-line CBs and may also impact the protection of a generator substation. Such attacks may cause disconnection of the generator substation from rest of the network and disable a specific interconnector between two areas, hence the power flow across the tie lines is affected.

3.2 Data integrity attack

The spurious injection attack in the form of data integrity attack can alter any control setting of the digital protection relays so that the protective devices operate wrongly. An external attacker hacks the protection and control algorithms of a digital relay through compromised communication channel. As a result, the perpetrator can gain control of the relay and manipulate the protection algorithms within the relay. This may cause unusual CB operation and make a line out-of-service, even if there is no physical disturbance.

According to the discussion above, integrity attacks can be modelled as the manipulation of relay pickup current settings,

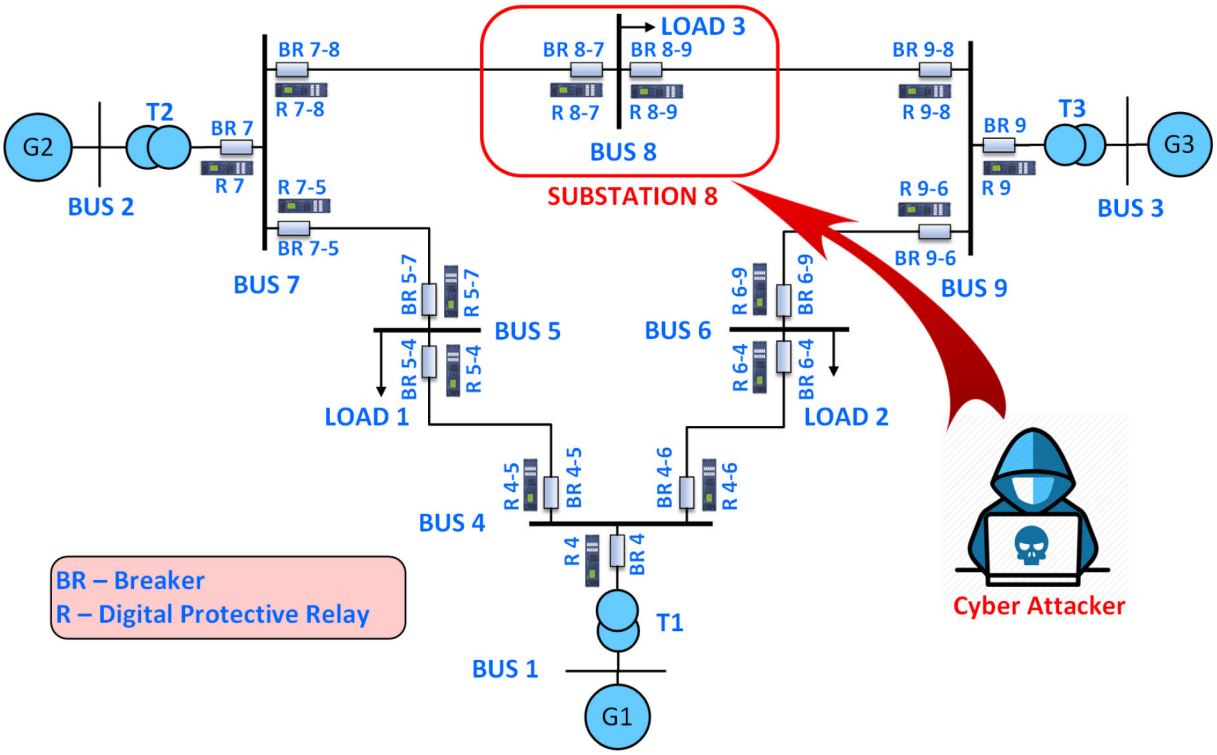

Fig. 3 *WSCC 3-machine 9-bus system*

which is used to determine the CB control or trip signal. If PS_i is the relay pickup current setting, the compromised setting can be written as

$$\bar{P}S_i = PS_i \pm PS_i^a \tag{10}$$

where $\bar{P}S_i$ is the compromised setting and PS_i^a is the injected spurious information by the attackers.

3.3 DoS attack

A DoS attack occurs when the attacker attempts to prevent or exploit the services of the relay from performing a necessary service. In this scenario, the attacker occupies excessive communication resources which in turn affects the availability of the captured information. This type of attack overwhelms a system's communication resources so that the system becomes unresponsive to other service requests. Two attack policies can be adopted here:

- Attack policy (1): In this case, DoS attack blocks the relay operation by transmitting malicious information to the targeted digital relays. The targeted attack compromises the transmission of control logic signal from the relays to the corresponding local CBs and permanently blocks the operation of protective devices during the event of credible contingencies. As a result, the control commands or breaker reclosing commands from the relay are not functioning as expected to mitigate the severity of the fault or disturbances. For example, due to this attack, the control logic (or reclosing instruction) cannot be transmitted to the local CBs to respond in any fault event.
- Attack policy (2): In this scenario, DoS attack keeps the relays in idle condition for a certain amount of time by preventing the relay from responding to any disturbance event. This type of attack may either prevent relay to immediately issue a trip signal to open CBs when there is a fault in the relevant section of the grid or create a delay to send control command to close/re-close the CBs when the fault is cleared.

3.4 Replay attack

A replay attack is a spurious strategy, in which a valid data is maliciously or fraudulently repeated. In the event of replay attacks, attackers can repeat the data recorded from a compromised database or data recorder for a certain time. In this scenario, attackers can gain remote access to penetrate the network information and may simply sniff the network traffic. They can record a set of previously occurred disturbance data, using perhaps a digital fault recorder (DFR), or compromising breaker status logs within a certain time interval. The attackers may resend the recorded information of the previous event to targeted network component to re-simulate that event, which may perform malicious tripping of CBs and lead to an unplanned power outage. Such an attack is difficult to detect without further examination of actual information and the resulting attack violates the timing constraints of CB operation. A simple mathematical model of relay attack on protection system can be presented as below.

Let $F_s(k) \in \bar{F}(k)$, where $\bar{F}(k)$ be the kth set of fault information stored in DFR. In the event of replay attack, the compromised set of DFR information can be written as

$$\bar{F}(k) \in f_k^a \tag{11}$$

where f_k^a is the compromised set of past information from the DFR, which could be a single fault status or multiple fault statuses.

4 Overview of the test grid

In this paper, the IEEE benchmark model of WSCC 3-machine 9-bus test system is considered for simulation and attack generation purposes (Fig. 3). Total 600 MW loads are connected to the system and two generators of 400 MVA, 20 kV (generator 2) and 250 MVA, 18 kV (generator 3) and one infinite bus are connected to support the power demand of the system. Infinite bus, generator 2 and generator 3 are connected to bus 1, bus 2 and bus 3, respectively. Two transformers of 400 MVA, 20 kV/230 kV and 250 MVA, 18 kV/230 kV are used for stepping up the generated voltage to the transmission line voltage. The base voltages are selected as 18, 20 and 230 kV. The 20 kV/230 kV transformer is connected between bus 2 and bus 7 and the 18 kV/230 kV transformer is connected between bus 3 and bus 9. The bus 8 is

connected to bus 7 and bus 9. CBs and relays are used to connect and disconnect loads and transmission lines on a bus. Advanced metering devices are embedded in relays at different substations to measure the voltages and currents, and generate tripping commands for the CB. In the model shown in Fig. 3, each distinct bus indicates a substation at which relays and breakers are connected. For instance, bus 8 belongs to the substation 8 and is considered as the remotely located substation which is vulnerable to cyber attacks. The attackers target the digital protective relay R 8–7 to initiate different types of cyber attacks and maliciously operate the CB BR 8-7. The overall system frequency is 60 Hz. A 300 MW load is connected to bus 8 and two 150 MW loads are connected to bus 5 and bus 6, respectively. Bus 7 is connected to bus 5 and bus 5 is connected to bus 4. Besides, the bus 9 is connected to bus 6 and the bus 6 is connected to bus 4. The load data and transmission line data are summarised in Tables 1 and 2. Rest of the system details are available in [23].

5 Dynamic impact analyses and recommendations

The IEEE benchmark WSCC 3-machine 9-bus test system is simulated in MATLAB/Simulink environment. One three-phase to ground fault and four types of cyber attacks such as random switching attack, integrity attack, DoS attacks and replay attacks are simulated in the system and the dynamic impacts of credible contingency and cyber attacks on the test system are investigated. The cyber attackers, as discussed in the previous section, manipulate the relays of critical pathways of vulnerable substations. Due to the malfunction of substation relays, the affected power system experiences an unexpected dynamic behaviour which may result in cascading failures and system blackouts. For the dynamic behaviour analysis, it is assumed that the attacker is able to compromise the operation of a single substation to comply with a practical availability of limited system's information to the attacker. The impacts of the three-phase to ground fault and different types of cyber attacks on system's dynamic performances are discussed in the following subsections.

Table 1 Load data

Bus no.	*P*, MW	*Q*, MVAR
5	150	48
6	150	48
8	300	16

Table 2 Transmission line data

Branch	*Y*, pu	*X*, pu	*R*, pu
4 to 5	0.079	0.092	0.017
4 to 6	0.079	0.092	0.017
6 to 9	0.179	0.17	0.039
5 to 7	0.153	0.161	0.032
7 to 8	0.0745	0.072	0.0085
8 to 9	0.1045	0.1008	0.0119

5.1 Impact analyses of credible contingency

The impact of three-phase to ground fault as the most severe type of contingency is analysed in this section. Protective relays are designed to sense the abnormal behaviour of the system by measuring the voltage and current fluctuations and sending commands to the CBs to clear the fault. In this paper, a three-phase to ground fault is created at bus 8 at 10 s and cleared at 10.2 s. The relay R 8-7 at the substation 8 senses the abnormal level of currents and voltages and sends a trip command to the CB BR 8-7. The dynamic parameters measured before, during and after the fault are presented in Fig. 4. The fault current at bus 8 rises up to 3000 A and the overcurrent relay R 8-7 immediately detects the abnormal situation. The tripping action is executed within 0.2 s which meets the standard practice for power system (Fig. 4*a*). The load angles of the generator 2 and generator 3 also drop drastically due to the sudden increase in the current (Fig. 4*b*). The three-phase voltages are dropped to zero during the fault (Fig. 4*c*) and recovered after clearing the fault. The generated active powers from the generators also increase and then return to their normal operating point after clearing the fault (Fig. 4*d*). As the results of the three-phase to ground fault in Fig. 4 show, all the currents, voltages, load angels of generators and the delivered powers are considerably fluctuated at the time of fault happening. Following that, the CT and/or potential transformer report such disturbances to the connected relays to protect the system via opening the CBs.

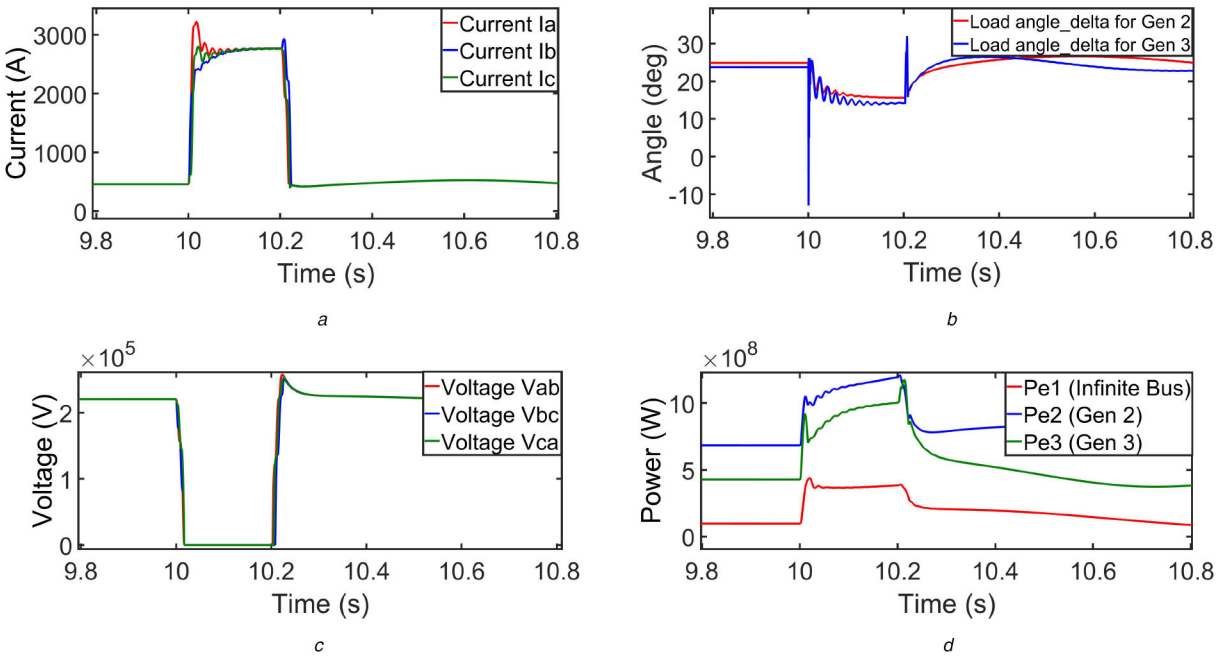

Fig. 4 *Dynamic parameters measured at substation 8 subject to three-phase fault at bus 8*

(a) Line currents from substation 8 to bus 7,

(b) Load angle variation measured at substation 8,

(c) Voltages measured at substation 8,

(d) Active power supply from generators 1, 2 and 3

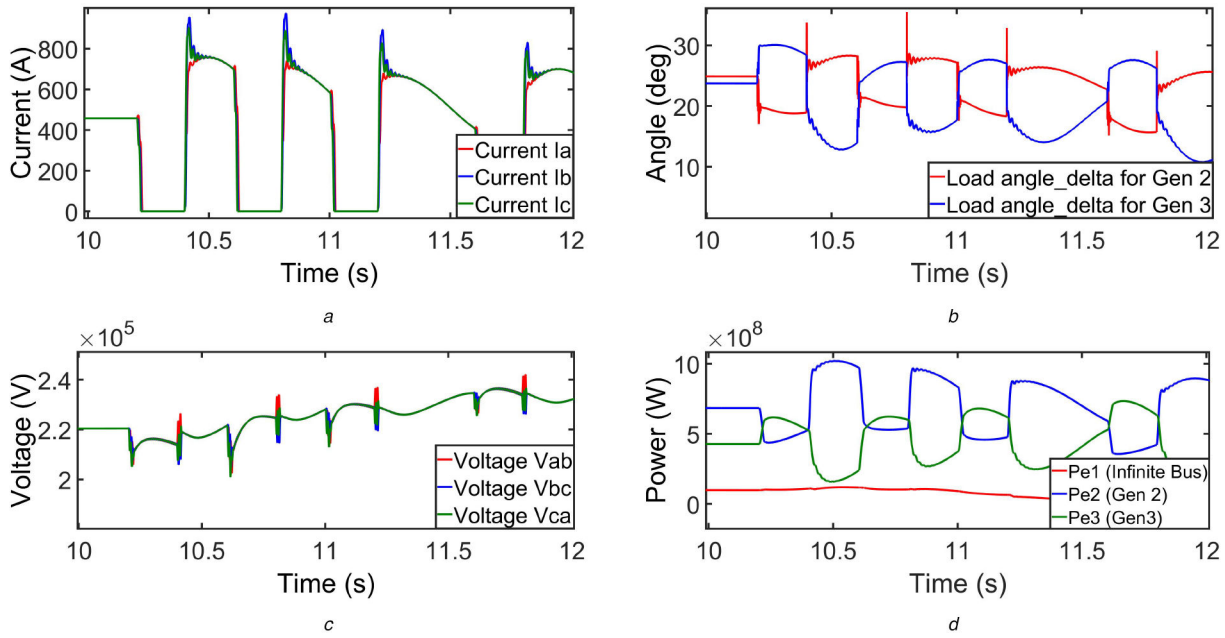

Fig. 5 *Dynamic parameters measured at substation 8 subject to the random switching attack at protection relay R 8-7*

(a) Line currents from substation 8 to bus 7,

(b) Load angle during random switching attack at relay R 8-7,

(c) Voltages measured at substation 8,

(d) Active power supply from generators 1, 2 and 3

5.2 Impact analyses of random switching attacks

A power system network can be operated remotely by system operators through communication channels. An attacker can gain access to the computer of a substation's relays or invade the communication channels to inject direct ON/OFF commands to a protection relay. The switching frequency of the CBs are chosen by considering the processing time delay of the relay and relay response time depending upon the current magnitude and curve selection [20]. The protection system of a traditional synchronous generator blocks the reclosing process for 15 cycles to ensure a proper synchronisation of the machine [3]. The attacker can manipulate this process and initiate random switching attack via compromising the communication channels.

In this section, a random switching attack is generated at the remotely located substation 8 and the variations of dynamic parameters are investigated. The attackers take control over the protective relay R 8-7 mounted on the substation 8 and send false switching ON/OFF commands to the CB BR 8-7 from 10 to 12 s within 10 cycle intervals. As a result of the continuous ON/OFF switching of BR 8-7, the line currents of the 8-7 transmission line severely fluctuate between 0 and 1000 A during OFF and ON period of the BR 8-7, respectively. The sudden in rush current measured by the relay R 8-7 is almost double than the operating current 460 A. The line currents during the switching attack are illustrated in Fig. 5*a*. As shown in Figs. 5*b* and *c*, load angles of the generators and three-phase voltages also fluctuate heavily due to the frequent ON/OFF switching of the BR 8-7 causing severe hunting effects to the generators and motors. Fig. 5*d* shows the output powers of the generators. During the OFF mode of the BR 8-7, the 300 MW load connected to the bus 8 is solely fed by the generator 3. As a result, generated power of the generator 2 decreases and the generated power of the generator 3 increases to meet the load's demand and vice versa.

In random switching attack, as explained, the CBs are falsely opened and closed for several times by the attacker. During this case, the relays would not be solely able to stop their opening/closing actions. However, if the relays are equipped with a real-time observer and able to observe the non-fault condition of the line current, voltage and/or frequency, they would be able to distinguish the attack and report it to the control centre to avoid further damages or blackouts.

5.3 Impact analyses of integrity attacks

A proper relay threshold setting is required to successfully detect fault situations in the system and generate trip command to the CB. Manipulating the threshold setting is an integrity attack. As the threshold is too high, overcurrent due to overload and short circuit faults may not be recognised by the relay and the CB may fail to trip during such abnormal situations.

Integrity attack is demonstrated in this section for the IEEE benchmark WSCC 3-machine 9-bus system described in Section 4. The nominal current flow through the line 8-7 is 460 A and the relay tripping threshold for short circuit current is set at 1200 A. In general, the physical security of remotely located substations are more vulnerable than the generating substations. Therefore, it is assumed that an attacker has compromised the setting of the relay R 8-7 at substation-8 via changing the current threshold from 1200 to 5000 A. A three-phase fault is applied to bus 8 at time 10 s and the protective relay R 8-7 fails to recognise the high level of inrush current of the fault because of the manipulated relay setting (Fig. 6*a*). As a result, the CB BR 8-7 continues to operate on ON mode and does not trip. Consequently, the fault remains in the system and the angles of the generators oscillate heavily (Fig. 6*b*) which can cause severe system instability. The generators' output powers also increase and cause severe overload to the generators as shown in Fig. 6*d*. The voltages at bus 8 remain zero due to the continuation of the fault (Fig. 6*c*) in the line 8-7.

5.4 Impact analyses of DoS attacks

A DoS attack is basically launched by delaying or blocking the switching command from a relay to a CB. During the DoS attack, the execution process of a relay's command in protection algorithm may be blocked, delayed or rejected. A successful DoS attack can cause devastating consequences to the system's performance and dynamic behaviours.

In order to illustrate a DoS attack scenario, a three-phase to ground fault is applied to the line 8-7 near to the bus 8 at 10 s. Although the overcurrent protection relay R 8-7 detects the overcurrent immediately, due to the DoS attack, the execution command has been delayed by 0.4 s and the CB BR 8-7 trips after 0.6 s. Such a delay violates the power system's standard and causes severe disruption on its dynamic behaviour. Basically, a 0.2 s delay is considered as the computational and communication delay to

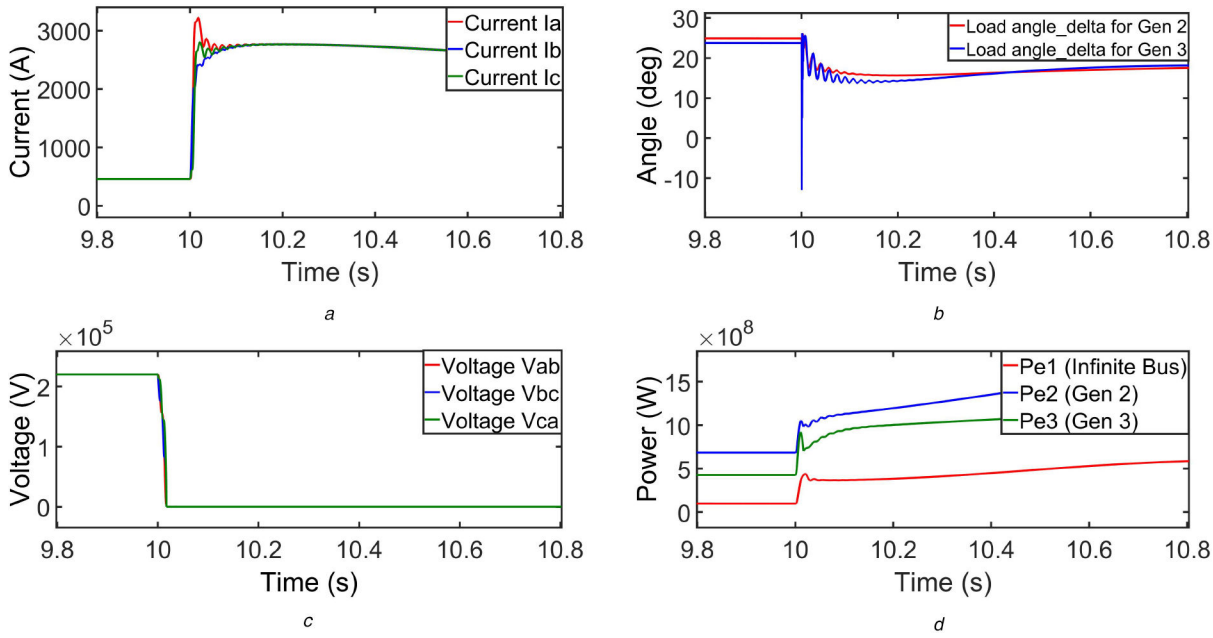

Fig. 6 *Dynamic parameters measured at substation 8 subject to the integrity attack at substation protection relay R 8-7*
(a) Line currents from substation 8 to bus 7,
(b) Load angle variation during integrity attack at relay R 8-7,
(c) Voltages measured at substation 8,
(d) Active power supply from generators 1, 2 and 3

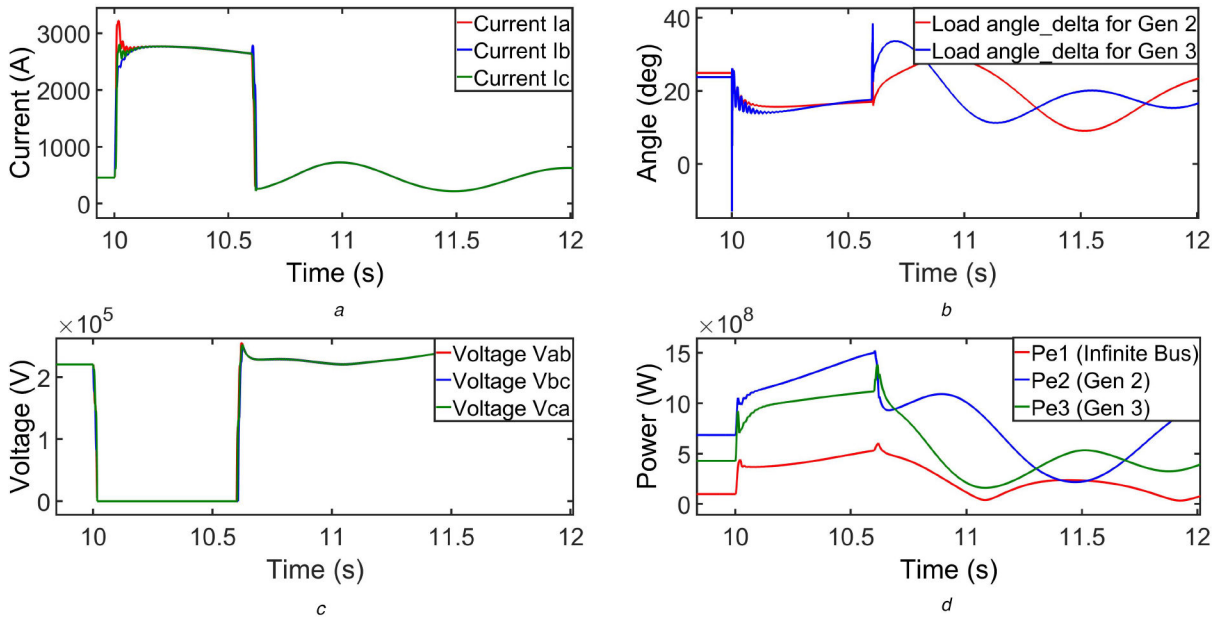

Fig. 7 *Dynamic parameters measured at substation 8 subject to the DoS attack at protection relay R 8-7*
(a) Line currents from substation 8 to bus 7,
(b) Load angle variation during DoS attack at relay R 8-7,
(c) Voltages measured at substation 8,
(d) Active power supply from generators 1, 2 and 3

execute the tripping command in power systems. As the fault remains more than the standard execution time (0.2 s), the system becomes more unstable than the normal clearing time [21]. The inrush current flowing through the transmission line 8-7 is shown in Fig. 7*a*. Comparing the dynamic behaviours of the system during DoS attack and the three-phase to ground faults in Fig. 4, the oscillations of generators' load angles (Fig. 7*b*) and output powers (Fig. 7*d*) are higher in DoS attack than the three-phase fault which is cleared within 0.2 s. Moreover, as Fig. 7*c* shows, the line voltages remain zero for a longer time until the tripping command is executed by the CB (Fig. 7*c*), which may cause severe damage to several electrical devices.

The same solution suggested for a random switching attack in Section 5.2 would be applied to distinguish data integrity attack or DoS attack scenario from normal fault condition. During these two attacks, the operational modes of the relays are manipulated by the attacker and thus cannot protect the system due to receiving a non-suitable setting, a blocking mode or a delay mode created by the attacker. Again, if the relays can recognise the falsified fault situations via observing the real-time dynamic of the network parameters, the attack can be understood by the control centres before causing damages or blackouts.

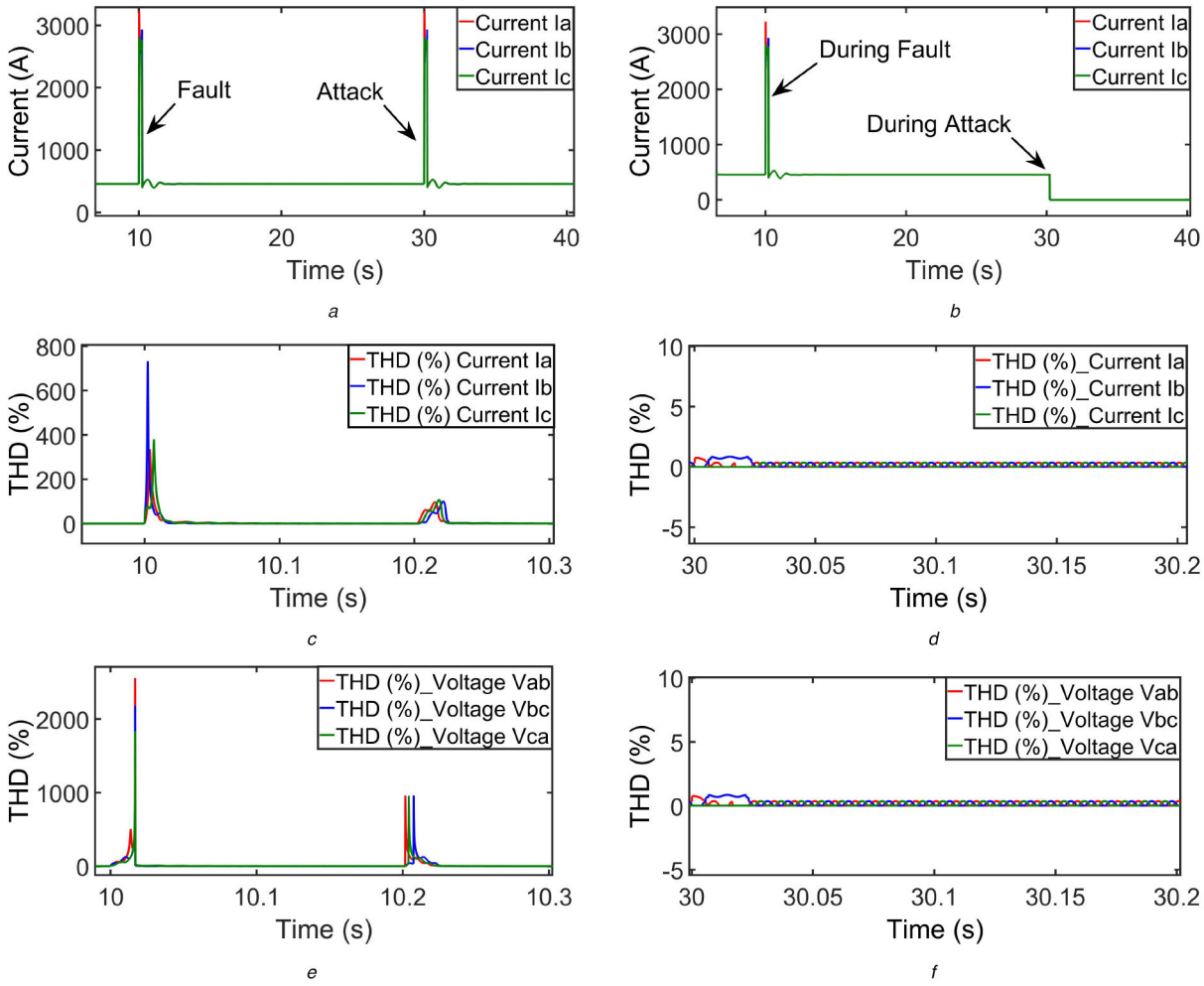

Fig. 8 *Dynamic parameters measured at substation 8 subject to the replay attack at protection relay R 8-7*

(a) Attacker current signal to the relay R 8-7,

(b) Actual line currents flowing from bus 8 to bus 7,

(c) THD of the line current during fault at bus 8,

(d) THD of the line current during replay attack to the relay R 8-7, ***(e)*** THD of the bus voltage during fault at bus 8, ***(f)*** THD of the bus voltage during replay attack at the relay R 8-7

5.5 Impact analyses of replay attacks

Replay attack in the power system protection system can be launched to deceive the protection measurement data processing and initiate an unnecessary and unscheduled tripping of the CB.

In this case, a three-phase fault is applied to the bus 8 at time 10 s and the fault is cleared at 10.2 s. It is assumed that the attacker is able to compromise the data acquisition module by gaining access to the communication channel. The attacker has stored the fault data from the data-acquisition module and replays this information to the relay at 30 s as can be seen in Fig. 8*a* which mimics the fault situation occurred at time 10 s. As a result, while there is no actual fault in the system, the relay opens the CB BR 8-7, and at 30.2 s, the line 8-7 is disconnected from bus 8 as depicted in Fig. 8*b*. The voltages, generator load angles and active powers delivered by the generators experience sudden topology changes. The replay attack may not be severe to a small single unit attack but could result catastrophic effect during coordinated attacks. The total harmonic distortion (THD) of the line current is very high (750%) during the fault but very low during the attack (1–2%) (Figs. 8*c* and *d*). The reason is that during the attack, there is no fault in the line and the current does not experience high THD. Similar results are also obtained for the bus voltage shown in Figs. 8*e* and *f*.

During a reply attack, while there is no real fault in the system and subsequently no disturbances on the currents, voltages, load angels of generators and delivered powers, a falsified fault scenario is sent to the relays by an attacker. If the protection system/scheme (i.e. relay) is able to observe the real-time dynamic parameters such as line currents, voltages and so on, they would be able to distinguish the fault condition from the attack scenarios, so that the unnecessary opening/closing CBs will be avoided.

Particularly for the replay attack where the attacker stores the data of a previous real fault condition and replays it back to the relay after passing a specific time interval, a THD-based alternative is recommended to be used. As can be seen in Figs. 8*c* and *d*, the THD of the line current is significantly different from the THD of the current during an attack. This could be a good indicator to distinguish the faults from attacks. As a future work of this research, a new real-time observer is aimed to be added to the relay. Accordingly, the relay will be able to measure the real-time THD of the line current and/or voltage and analyse the situation. Following that, if a falsified fault command is received from the attacker, while the line current and/or voltage exhibit normal THD condition, the attack can be identified quickly, best actions can be adopted and the reports are sent to the control centre, thus potential damages/blackouts can be avoided.

6 Conclusion

This paper presents a novel approach of analysing the dynamic behaviour of a power system during four types of cyber attacks, i.e. random switching attack, integrity attack, DoS attack and replay attack. The system's dynamic performance during normal fault is also shown and the related dynamic-based recommendations are proposed accordingly. The dynamic analysis has the advantages of considering the variation of more system parameters such as line current, voltage, load angle of generators, delivered power and frequency which are always assumed to be constant in steady-state analysis. Moreover, the dynamic analysis can cover more system's

perturbations as well as post-disturbance behaviours. As the dynamic performance of power grids during cyber attacks is quite distinctive than that of during physical short circuit faults, therefore detection and protection measures based on system dynamic behaviour are highly recommended alongside the conventional steady-state analysis and IT-based security.

7 Acknowledgment

The authors acknowledge the NSW Cyber Security Network, Australia for financial support.

8 References

[1] He, H., Yan, J.: 'Cyber-physical attacks and defences in the smart grid: a survey', *IET Cyber-Phys. Syst., Theory Appl.*, 2016, **1**, (1), pp. 13–27

[2] AEMO: 'Australian energy sector cyber security framework education workshop', October 2018

[3] Zeller, M.: 'Myth or reality – does the aurora vulnerability pose a risk to my generator?'. 2011 64th Annual Conf. for Protective Relay Engineers, College Station, TX, USA., 2011, pp. 130–136

[4] Liang, G., Weller, S.R., Zhao, J., *et al.*: 'The 2015 Ukraine blackout: implications for false data injection attacks', *IEEE Trans. Power Syst.*, 2017, **32**, (4), pp. 3317–3318

[5] Gurevich, V.: '*Cyber and electromagnetic threats in modern relay protection*' (CRC, Boca Raton, FL, USA, 2017)

[6] Liu, Y., Ning, P., Reiter, M.K.: 'False data injection attacks against state estimation in electric power grids', *ACM Trans. Inf. Syst. Secur.*, 2011, **14**, (1), pp. 1–33

[7] Zhang, J., Chu, Z., Sankar, L., *et al.*: 'Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?', *IEEE Trans. Power Syst.*, 2018, **33**, (5), pp. 4775–4786

[8] Deng, R., Xiao, G., Lu, R.: 'Defending against false data injection attacks on power system state estimation', *IEEE Trans. Ind. Informat.*, 2017, **13**, (1), pp. 198–207

[9] Li, Y., Wang, Y.: 'False data injection attacks with incomplete network topology information in smart grid', *IEEE Access*, 2019, **7**, pp. 3656–3664

[10] Wang, Q., Tai, W., Tang, Y., *et al.*: 'Review of the false data injection attack against the cyber-physical power system', *IET Cyber-Phys. Syst., Theory Appl.*, 2019, **4**, (2), pp. 101–107

[11] Liang, G., Zhao, J., Luo, F., *et al.*: 'A review of false data injection attacks against modern power systems', *IEEE Trans. Smart Grid*, 2017, **8**, (4), pp. 1630–1638

[12] Kim, J., Tong, L.: 'On topology attack of a smart grid: undetectable attacks and countermeasures', *IEEE J. Sel. Areas Commun.*, 2013, **31**, (7), pp. 1294–1305

[13] Choi, D., Xie, L.: 'Economic impact assessment of topology data attacks with virtual bids', *IEEE Trans. Smart Grid*, 2018, **9**, (2), pp. 512–520

[14] Liang, G., Weller, S.R., Zhao, J., *et al.*: 'A framework for cybertopology attacks: line-switching and new attack scenarios', *IEEE Trans. Smart Grid*, 2019, **10**, (2), pp. 1704–1712

[15] Ameli, A., Hooshyar, A., El-Saadany, E.F.: 'Development of a cyber-resilient line current differential relay', *IEEE Trans. Ind. Inf.*, 2019, **15**, (1), pp. 305–318

[16] Hong, J., Nuqui, R.F., Kondabathini, A., *et al.*: 'Cyber attack resilient distance protection and circuit breaker control for digital substations', *IEEE Trans. Ind. Inf.*, 2019, **15**, (7), pp. 4332–4341

[17] Liu, X., Shahidehpour, M., Li, Z., *et al.*: 'Power system risk assessment in cyber attacks considering the role of protection systems', *IEEE Trans. Smart Grid*, 2017, **8**, (2), pp. 572–580

[18] Johnson, J., Quiroz, J., Concepcion, R., *et al.*: 'Power system effects and mitigation recommendations for der cyberattacks', *IET Cyber-Phys. Syst. Theory Appl.*, 2019, **4**, (3), pp. 240–249

[19] Ten, C.W., Yamashita, K., Yang, Z., *et al.*: 'Impact assessment of hypothesized cyberattacks on interconnected bulk power systems', *IEEE Trans. Smart Grid*, 2018, **9**, (5), pp. 4405–4425

[20] Rahman, M.S., Mahmud, M.A., Oo, A.M.T., *et al.*: 'Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems', *IEEE Trans. Ind. Inf.*, 2017, **13**, (2), pp. 436–447

[21] Rebizant, W., Szafran, J., Wiszniewski, A.: '*Digital signal processing in power system protection and control*' (Springer Publishing Company, New York, USA., 2011)

[22] NERC: 'Misoperations report'. Protection System Misoperations Task Force-NERC Planning Committee, 2013

[23] Sauer, P.W., Pai, M.A.: '*Power system dynamics and stability*' (Prentice Hall, Upper Saddle River, NJ, USA., 1998)