



# Dynamic Security Assessment for Power System Under Cyber-Attack

Qusay A. Al-Gburi<sup>1</sup> · Mohd Aifaa Mohd Ariff<sup>1</sup>

Received: 14 December 2017 / Revised: 15 August 2018 / Accepted: 23 November 2018 / Published online: 15 January 2019  
© The Korean Institute of Electrical Engineers 2019

## Abstract

In recent years, power systems have become more dependent on new technological advancement in the communication network to send and receive data and commands through the wide area power network. This dependence has created a new threat to the network, known as a cyber-attack. Such attacks could lead to blackouts and the consequences on the security of the power system would be severe. This study presents a new approach, which aims at assessing the dynamic behavior of the test system's model under a cyber-attack contingency. The methodology used in this study was based on the scenarios of cyber-attacks on the protection relay devices to generate the database for dynamic security assessment. Then, a data mining framework was used for the database preparation and classification via feature selection algorithm and decision tree classifier. The results of the modified IEEE 30-bus test system model in this study showed a high accuracy of 99.537%, and a short time frame that makes this application suitable for real-time application to protect the power network from an insecure state and ensure that the power system remains reliable.

**Keywords** Dynamic security assessment · Cyber-attack · Decision tree · Logistic model trees · Symmetrical uncertainty

## 1 Introduction

The power system network has been continuously developed for over the last few decades. The network has become more extensive and complex, equipped with a huge and highly sophisticated communication network to meet the rapid increase in load demands. In order to manage and control the network, different media and transfer protocols, have been used. The high integration of communication technology into the power grid and the implementation of intelligent devices have caused the power grid to become more vulnerable to a new threat known as cyber-attack. Cyber-attack is defined as a suspicious intention of an attacker (e.g. hacker) to illegally obtain private information from computer networks or individual personal computers connected to the internet for the purpose of stealing or damaging the targeted information [1]. The impact of a cyber-attack on a power

system is detrimental to both the electric companies and users. This is because the cyber-attackers have the ability to cause direct impact on the transmission of power in the electrical grid.

Recently, the motivation and number of cyber-attacks have increased due to the benefits gained by the attackers from these non-individual attacks. This kind of attack is usually motivated by the ideology adopted by the attackers such as terrorism, or political conflicts. As an example, the Ukraine blackout in December 2015 was due to a confirmed cyber-attack [2]. In 2009, China and Russia made attempts to penetrate the power system network in the United States of America [3].

The cyber-attackers could collect information about the power grid topology using open source online maps or commercially available drones. Typically, cyber-attackers would start with a reconnaissance attack to identify the login keyword and the protocols used for sending and receiving information through various communication networks. For power system network operation, the control center uses a secure communication tunnel, known as the virtual private network (VPN) to interact with intelligent electronic devices (IED) through the wide area networks (WANs) and the local area networks (LAN) to control the procedures for daily operations, maintenance, and control. However, the attackers

✉ Qusay A. Al-Gburi  
qusay\_75@yahoo.com

Mohd Aifaa Mohd Ariff  
aifaa@uthm.edu.my

<sup>1</sup> Department of Electrical Power Engineering, Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn, 86400 Parit Raja, Malaysia

could gain access to the VPN via a keylogger or Trojan virus. Consequently, the attackers could pass the firewall and take over control from the respective utility company. Although the control center has also used strong encryption for network traffic (e.g. secure sockets layer (SSL) [4]) to deal with such an attack, not all communication networks or electrical devices could be secured by this encryption technology especially at the distribution system communication network. Recently, even a highly secure encryption algorithm utilized in Wi-Fi Protected Access 2 (WPA2) is hacked by the irresponsible personnel [5]. Therefore, there is no Wi-Fi network in the world can ever be considered secure anymore.

According to researchers in [6], cyber-attacks can be considered as another type of power system contingencies. These attacks could lead to large-scale blackouts [7–9] because they are often carefully planned events to cause maximum damage. In fact, a cyber-attack could affect many parts of the power system based on the type of attack and the target region. There are several means of cyber-attacking the power grid. One of the most effective ways to do this is by using the false data injection attack [10]. This type of attack is regarded as the most effective attack due to its economical aftermath impact on the utilities and society. In this attack, the attacker will send fake commands into the network to disrupt the power system's devices and controls. Consequently, the false injection attack causes a "butterfly effect" which would have aggravated the impact of disturbance to the overall power grid. The attack could falsely trigger the operation of critical protection element at the weak transmission line links in the power network. The relay false operation may weaken the network and initiate cascading failures throughout the network. Eventually, the sequence of the event may lead to the catastrophic wide-area blackout.

In order to study the reaction of the power grid against the false data injection attack, it is vital to first examine the effects of cyber-attack contingencies on the power system via DSA. The DSA evaluates the security status based on the power system behaviors (either secure or insecure) following a contingency in the system. Traditionally, the study of DSA is based on normal contingencies that arise from lightning, normal failure of the protection devices, and overload. However, with the increasing probability of cyber-attacks on the power grid, the control center should now develop a better defense strategy to protect the power system against this new threat. Cyber-attack contingencies should be included and considered in the simulations and analyses of the system dynamic security.

In the literature, numerous researchers have focused either on the modeling or the detection of the cyber-attack itself [6, 11, 12]. However, none of these studies have directed their attention to the impact of cyber-attack on DSA. The outcome from the DSA dictates the performance of power

system control and operation. As the DSA is vulnerable to the cyber-attack, it is vital to study, analyze, and come out with an elegant solution to address this challenge. In this paper, a new study is discussed to represent and analyze the impact of cyber-attack contingency on the power system on the performance of the DSA tool. Consequently, a new DSA approach is developed to assess the dynamic security of the system following cyber-attacks contingencies. The proposed approach is based on a logistic model tree classifier and symmetrical uncertainty methods. The proposed solution is an accurate and fast classifier that can assess the dynamic security state under normal and cyber-attack contingencies. In order to demonstrate the effectiveness of the proposed method, the performance of the method is compared with other classifier technique in assessing the dynamic security of the system.

The remainder of this paper is organized as follows. Section 2 discusses the recent trends in the DSA analysis and technique. Then, Sect. 3 explains the contingency from the point of view of the protection relays. The proposed methodology is presented in Sect. 4. Next, the results, analyses, and discussion of the proposed method are presented in Sect. 5. Finally, the conclusion and future recommendations are discussed in Sect. 6.

## 2 State-of-the-Art

Conventionally, DSA was developed based on the heuristic assumption of the system's operating situation and load demand forecasting [13]. This type of analysis is based on a standard assessment of the contingency involved in power system the daily operation. The evaluation process is realized by considering a collection of the most apparent and critical contingencies during the normal daily procedure. However, it is well known that this conventional method is slow and time-consuming. Therefore, power system researchers and engineers proposed a data mining technique to address this issue. Data mining technique could build a learning system model to discover the relationship between different input information and output results with high accuracy and in the shorter time frame.

Data mining has many successful applications in various scientific fields [14]. Many data mining algorithms have been used for DSA, such as artificial neural network (ANN) [15–17], fuzzy logic (FL) [18, 19], decision tree (DT) [20–24], extreme learning machine (ELM) [25], and support vector machine (SVM) [26]. Although these techniques have addressed the predicament of the conventional DSA, there is still so much room for improvement, especially for real-time DSA application. In the literature, the DT method shows higher efficiency and less computer time, especially when dealing with a significant amount of data as compared

to other data mining method. These advantages made it suitable for the online DSA applications. Inside the DT, various algorithms could give different results in terms of accuracy and computational time, as shown in [26]. Researchers in [27, 28] employ a hybrid system involving two different algorithms to improve their results. These combined algorithms show superior performance as compared to the standalone data mining methods.

A critical issue that needs to be given priority in data mining is the training stage; this is the stage where the classifier algorithm is trained to uncover the relationship between the input data (measurement) and the output result (secure state). This process depends on the type of data in which the classifier is being trained. It can also increase the number of instances for the dataset, which could provide more discriminating classifier power [29]. Thus, the increasing threat of cyber-attacks and the limitations of the traditional defense and analysis strategies currently utilized for the control center show the urgent need for more training to cater to the different types of contingencies related to cyber-attacks. In other words, cyber-attack contingency must be considered in the training of data mining classifier for DSA. Only then, the classifier could distinguish the security state of the new cases in the dataset and offers the right assessment to the control center, so the right steps can be taken to protect the power system.

The focus of this study is to develop a robust DSA classifier that can accurately assess the dynamic security of the system even if it is under cyber-attack. In order to achieve this aim, cyber-attack contingencies need to be considered in developing the training dataset for the DSA classifier. Consequently, the size of the training dataset will increase significantly with this added consideration. This increment may affect the performance of the DSA classifier. The proposed method utilizes a symmetrical uncertainties algorithm to significantly reduce the training data dimension for logistic model trees algorithm to assess the dynamic security assessment of the system. The explanation on representing the cyber-attack contingency and methodology used in this study will be explained in the following sections.

### 3 Contingency via protection relays

The contingency simulation and analysis technique investigate the risk of the power system in terms of security and reliability. Utility operation planning should confirm that the power system could maintain stability and operates within the acceptable limits following the N-1 and N-2 contingencies [26, 30]. Currently, these contingencies are based on normal contingencies, such as faults, or equipment failure, but not on cyber-attack contingencies. However, if the cyber-attack targeted the power components, such as the protection

relays, then the influence of this attack could be similar or even more damaging than that of N-1 and N-2 contingencies.

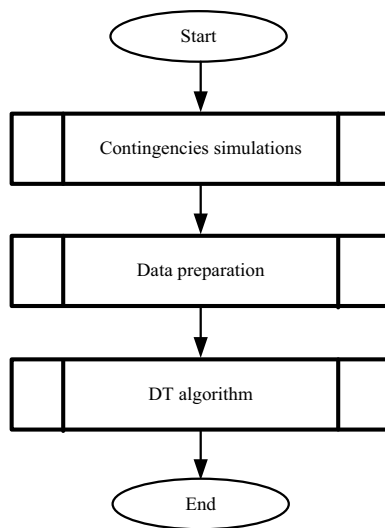
The protection relays are responsible for opening and closing the line to protect the system from the abnormal operating condition. If the cyber-attacker could have access to the protection relay operation, then the cyber-attacker could open one or more transmission lines. Based on practical experience, any false-operation of the protection relay could be costly to the system operation. Based on the North American Electric Reliability Council (NERC) report, the mal-operation of protection relays is responsible for more than 70% of the major contingencies in the USA [31, 32]. The false-operation of the protection system could initiate the cascade-tripping of other protection relays, and consequently a wide-area interruption of the power service [33].

With the development and expansion of IED in the power networks [11], the control center uses MODBUS/TCP protocol to effectively control the protection relays and remote monitors as well as the trips [12]. Moreover, IED has included the phasor measurement unit (PMU) function to measure the state of transmission lines [12]. The PMU used for data streaming open standard protocols include the IEEE C37.118 standard with low-security features [11]. Even this technology has improved the performance of the system operation, this advancement of the control and protection have left the power system operation vulnerable towards cyber-attack.

### 4 Proposed Methodology

To achieve the research objective, this methodology is divided into three stages: (1) contingencies simulations, (2) data preparation, and (3) DT algorithm. The proposed methodology to evaluate the dynamic security of the system under normal and cyber-attack contingencies are presented in Fig. 1. In contingencies simulation stage, dynamic simulations are performed to determine the system's behavior under normal and critical cyber-attack contingencies. Next, the responses from the system for all contingencies are utilized in data preparation to form the training dataset for the DT. Finally, the dataset is utilized in stage three where the symmetrical uncertainties will reduce the data dimension by minimizing data redundancy in the dataset. Logistic model tree algorithm will use the reduced dataset to assess the dynamic security status of the system following a contingency in the power network.

In this study, the dynamic behaviors of the modified IEEE 30-bus test system model under normal and cyber-attack contingencies are simulated. The system responses under normal and cyber-attack contingencies are combined into one large dataset. This assumption is considered because the cyber-attackers would usually try to replicate



**Fig. 1** The main flowchart of the proposed methodology

an attack scenario that is close to or has a similar characteristic with the normal contingencies cases to learn the corresponding responses from the control center. This kind of attack is also performed by the cyber-attacker to discover the way to avoid detection and evaluate the probability of success rate. Therefore, combining these two types of contingencies offer many practical and logical advantages. For the contingencies simulation stage, only N-1 and N-2 contingencies are considered as the normal contingency scenarios. As for the cyber-attack scenario, the number of cases involved will depend on the number of buses in the test system model. The assumption considered as the cyber-attack here is that the cyber-attacker has access to the protection relays that are supposed to protect the corresponding transmission lines. The cyber-attack scenario is applied at one of the buses in the test system model and the system responses are recorded. This simulation of the cyber-attack scenario is repeated for all other buses to ensure that the dataset will consist of all possible scenarios. This implies that the cyber-attacker could only attack one bus at a time. This assumption of

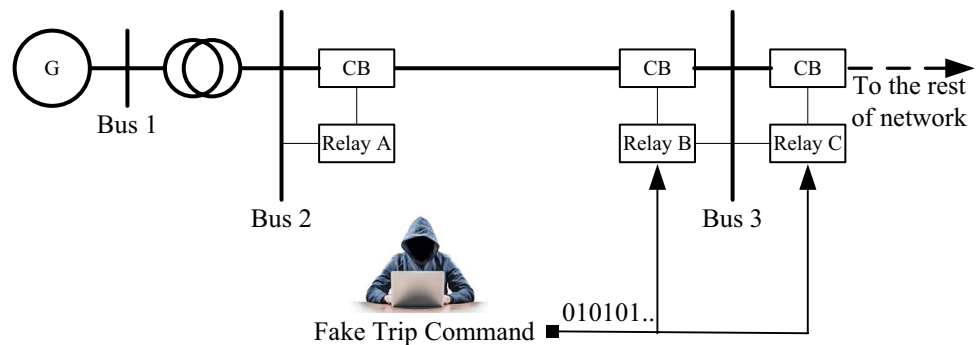
scenario is based on the heuristic assumption of a cyber-attack in practice.

Figure 2 illustrates the typical scenario of a cyber-attack contingency. From the figure, it shows that the attacker could send a fake trip command to the protection relays B and C that are connected to Bus three. Consequently, the relay will send a false tripping signal to open the circuit breakers (CB).

In the smart grid architecture, the control center could remotely change the settings of the protection relay in the system for operation or maintenance purposes. Also, the control center could control the operation of the circuit breaker remotely. Therefore, the attacker would try to use this communication path to gain access to the protection relay and circuit breaker in the system. The cyber-attackers could penetrate the communication network via various technical hacks, such as creating a spoofed IP address to capture the information in the network traffic, specifically in the MODBUS/TCP protocol. Then, the cyber-attackers could use their computer to remotely change the settings of the protection relays or directly send the trip command to the circuit breaker. This attack will cause the CB to false-operate and may initiate cascading tripping in the signal. Even worst, this attack will not be recorded in the panel log of the control center since this command is not sent from the panel's computer belonging to the control center. Thus, the control center may not be able to recognize this type of contingencies. The following scenario is used to represent the cyber-attack contingency in the simulation stage:

1. The applications of a balanced three-phase fault for 0.1 s at all the transmission line while keeping the load within normal limits (47 cases).
2. A transmission line is open at a normal load and then at 110% load (94 cases).
3. Two transmission lines are open at the same time near the generation busses for a normal, 110% and 120% loads (45 cases).
4. At a normal load in every single bus, in which the cyber-attack scenario was applied, all the transmission lines connected to this bus are open at the same time (30 cases).

**Fig. 2** Flowchart of a cyber-attack contingency



**Table 1** Opened transmission lines in scenario three

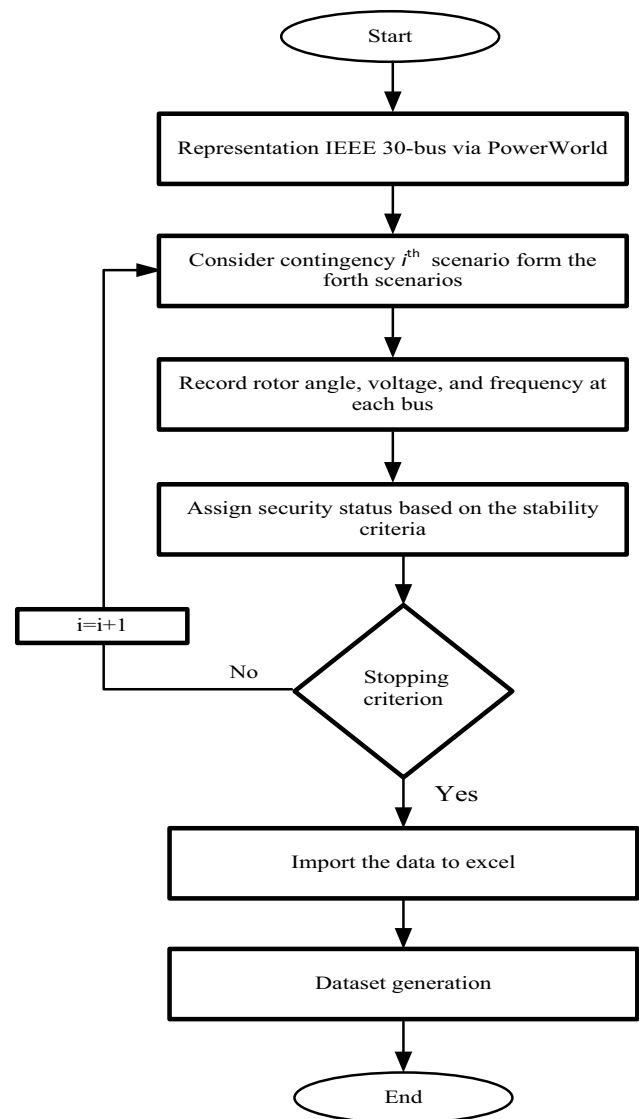
Case no.	Opened transmission lines
1	1–31 & 13–36
2	1–31 & 8–34
3	1–31 & 5–33
4	1–31 & 2–32
5	1–31 & 11–35
6	2–32 & 13–36
7	2–32 & 8–34
8	2–32 & 5–33
9	2–32 & 11–35
10	13–36 & 8–34
11	13–36 & 5–33
12	13–36 & 11–35
13	8–34 & 5–33
14	8–34 & 11–35
15	5–33 & 11–35

For scenarios one and two, the cases represent the sum of numbers of the transmission lines. On the other hand, scenario three represents two lines opened near the generators at the same time and three different cases of load, i.e. normal load, 110% of normal load, and 120% of normal load. The reason for that can be detailed in the Table 1.

Next, three stability criteria, namely the rotor angle, voltage, and frequency for each bus are recorded after each contingency is subjected to the power system model. The secure state operation limits for DSA, based on the rotor angle, voltage, and frequency, are as follows:

1. If the rotor angle, which is the maximum angle of separation of any two synchronous generators in the power system during the post-disturbance, is less than  $180^\circ$ , the system is secure.
2. If the voltage ranges between  $0.9 \leq V \leq 1.0$  per unit, the system is secure.
3. If the frequency ranges between  $49.5 \leq f \leq 50.5$  Hz, the system is secure.

If these three measurements limits are not fulfilled, the system is indicated as insecure. Figure 3 summarizes the process of dataset generation for the DSA method proposed in this paper. Following the contingencies simulation, the generators rotor angle, voltage, and frequency are measured for all contingencies. Each contingency will be assigned with its security status in accordance with their respective security limit. Next, the dataset is processed by incorporating supplementary features labels such as name, value, and type. This process is necessary in order to distinguish the element in the dataset. Consequently, the proposed method is applied to the dataset to train the

**Fig. 3** The contingencies simulations and dataset generation

classifier to assess the dynamic security of the test system model.

To ensure a successful classification process, the dataset needs careful preparation to enhance the quality of the dataset. This is realized by removing the noise and reducing redundant and non-relevant features in the dataset. All these data preparation processes are summarized in the second stage of Fig. 1. An advanced feature selection technique based on symmetrical uncertainty algorithm is utilized in this study to perform the dataset preparation for the proposed DSA method.

Advanced feature selection is one of the data mining techniques based on mathematical analyses on the dataset. It is used to select only high-ranking features throughout the whole dataset. The main benefit of this technique is it can simplify and reduce over-fitting issue in a dataset so

that it is easier for the classifier to interpret the dataset. In the literature, this technique has improved the accuracy of the data mining classifier and reduce the time required to perform its task [29]. This is because the advanced feature selection technique is able to clarify the features and significantly reduce the size of a dataset while maintaining the important features in it.

Symmetrical uncertainty plays a vital role in analyzing and enhancing the parameters of the features in a dataset, especially for data mining method [34, 35]. There are two major advantages of this technique. First, it is proficient to explore the features in a dataset. Second, it can map and organize the dataset from high to low while considering all the necessary and possible structures.

Symmetrical uncertainty algorithm depends on the concept of entropy that measures the uncertainty of random variables [36]. To represent the entropy of a given variable  $X$ , this formula is used:

$$H(X) = - \sum_i P(x_i) \log_2 (P(x_i)), \quad (1)$$

where  $P(x_i)$  is the previous probability for all values in the vector  $X$ . As a result, the entropy of  $X$  after observing values of a different variable  $Y$  can be defined as:

$$H(X|Y) = - \sum_j P(y_j) \sum_i P(x_i|y_j) \log_2 (P(x_i|y_j)), \quad (2)$$

where  $P(x_i|y_j)$  is the probabilities of  $X$  for a given vector  $Y$ . The subtraction of entropy in  $X$  provides additional information about  $X$  provided by  $Y$ , the resulting value is called information gain ( $IG$ ) and it is described as:

$$IG(X|Y) = H(X) - H(X|Y) \quad (3)$$

According to Eq. (3),  $Y$  is more correlated to  $X$  than to  $Z$ , where  $IG(Z|Y) < IG(X|Y)$  considering that  $X$  is symmetrical to  $Y$ . Features with higher  $IG$  values have a tendency to reduce errors between the classification labels and non-relevant features within the dataset. The SU algorithm is used to normalize  $IG$  with the corresponding entropies as follows:

$$SU(X, Y) = 2 \left[ \frac{IG(X, Y)}{H(X) + H(Y)} \right] \quad (4)$$

The value of  $SU$  falls in the vector  $[0, 1]$ , where  $SU=0$  means that there is no correlation and that features  $X, Y$  are independent. A value of  $SU=1$  means that features  $X, Y$  are highly correlated. This method is utilized to reduce the dimension of the dataset by selecting only relevant features.

Following the application of symmetrical uncertainty, the dataset is fed into the decision tree classifier. The classifier is an instrument to scaffold the procedure of decision-making for the dynamic security assessment technique of the system. The scaffolding is achieved by modeling the choices with their feasible results in the form of a tree-like graph.

The decision tree classifier has root and branch, and the root expands to a branch with the corresponding features. Subsequently, two subsets of outcomes will emerge from each branch that is constructed from the traits that have been ascertained earlier in the higher-level branch. This procedure is regenerated pending for the desired level of outcomes. The results that emerge at every level are characterized by the nodes. In this study, the desirable level of the result is depended on the traits that determine whether the system can be considered as insecure or secure. This process is an effectively administered data mining instrument created to resolve high-dimension setbacks in data classification. Nevertheless, a collection of database involving different case studies is needed to operate the decision tree algorithm.

This research uses Logistic Model Tree (LMT) algorithm to classify whether the system is secured or not following a disturbance in the system. In the literature, LMT has been used over a myriad of application ranging from weather to the customer behavior prediction and medical applications [37–39]. While following the decision branches in the tree algorithm, LMT replaces the terminal nodes with logistic regression functions [40]. As the regression analysis creates a relationship between a dependent variable and independent variables, LMT carries out a predictive analysis. The inclusion of the regression analysis in the decision tree algorithm enables the extraction of the class probabilities rather than simply getting the class assignments. Consequently, this variation transforms the conventional decision tree into a more comprehensive classifier. As the result, it has a comparatively higher accuracy as compared to the conventional decision tree algorithm.

To build the classifier model, the LMT classifier is applied to the reduced dataset. In this application, this dataset is segregated into two sets of datasets; a training set and a testing set that are used in the training and testing process of the classifier, respectively. In the training process, LMT tries to discover the relationship between the input features (measurements) and the output (security state). This process is followed by the testing process which tries to validate the classifier model built using the training dataset. If the performance of the test is satisfactory, the LMT classifier model will be used to assess the dynamic security of the system. Otherwise, the classifier model needs to undergo these processes recursively until the performance of the classifier is satisfactory for DSA application. This study uses WEKA as the data mining program [29].

## 5 Results, Analyses, and Discussions

The methodology described in this paper is applied to the modified IEEE 30-bus test system model. The test system model consists of 36 buses with the total load demand of

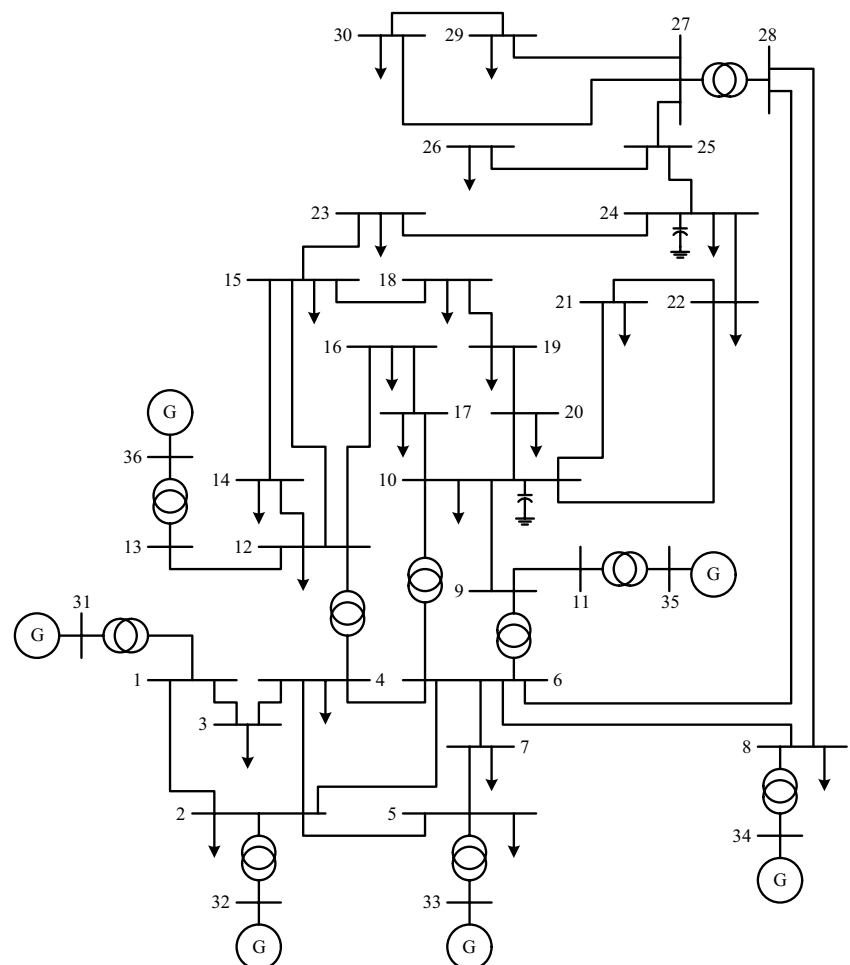
active and reactive power are 283.4 MW and 126.2 MVAR, respectively [41]. Table 2 summarizes the number of critical elements in this test system model. Figure 4 shows the single line diagram of the system.

In this paper, PowerWorld simulator [42] program are used to simulate normal and cyber-attack contingencies on the test system model. To study the system dynamic behavior for dataset construction; rotor angle, bus voltage, and frequency are measured following a contingency in the system. Based on the methodology described in Sect. 4, there are 216 contingency scenarios considered in this study. For each contingency, there are six measurements of the generator

**Table 2** Information on the modified IEEE 30-bus

Components	Number
Synchronous compensators	6
Buses	36
Transmission lines	37
Transformers	10
Constant impedance loads	21

**Fig. 4** Diagram of the modified IEEE 30-bus system



rotor angles and 36 measurements of the bus voltage and the bus frequency, respectively. Subsequently, security status tags are added at the end of each row of data to define the security state of the system following the corresponding contingency. The status is set to either “1” if the system is secure, or “0” if the system is insecure. From the simulation of these contingencies, there are 144 cases that are tagged with the security state of “1”, and 72 cases that are tagged with the security state of “0”. This implies that the dimension of the dataset for DSA following all contingency scenarios consist of  $78 \times 216$  features.

Figure 5, 6 and 7 show the rotor angle, bus voltage and bus frequency responses of the system following the intrusion of the cyber-attacker in the system network. The severity of this attack can be seen in these figures. From Fig. 5, the rotor angle of generator 34 oscillates out-of-step with other generators in the system almost instantaneously. The difference between the rotor angles for the generators (generator 34 w.r.t other generators) after the contingencies occur at  $t = 1.0$  s is more than  $180^\circ$  almost instantaneously. The difference continues to increase exponentially

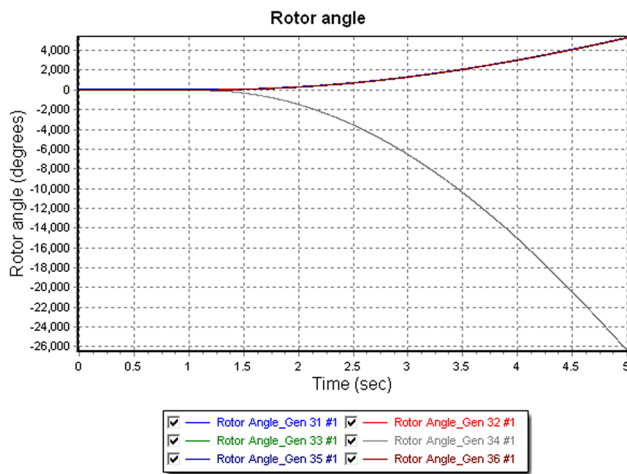


Fig. 5 Insecure generators’ rotor angle responses for server cyber-attack contingency scenario on bus six

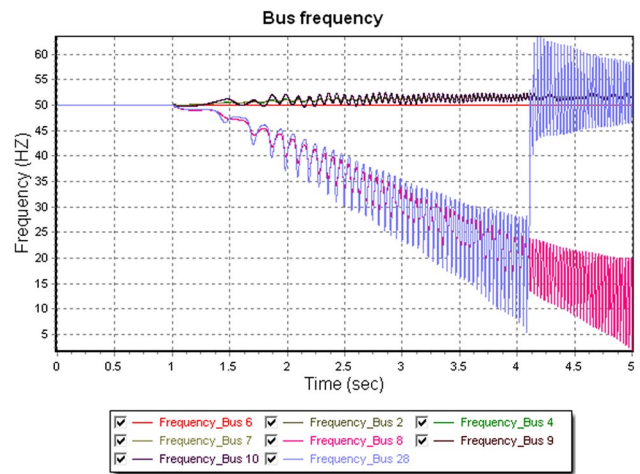


Fig. 7 Insecure frequency responses for server cyber-attack contingency scenario on bus six

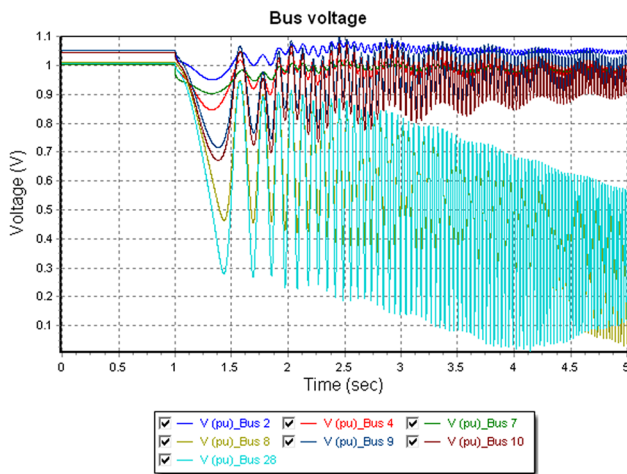


Fig. 6 Insecure bus voltage responses for server cyber-attack contingency scenario on bus six

with time and this could cause catastrophic physical damage to the generators if it is not rectified immediately.

Figure 6 shows the bus voltage responses of all buses that are directly connected to bus six. The figure illustrates that the oscillation of the voltage magnitude increased exponentially following the cyber-attack contingencies at  $t=1.0$  s. Eventually, the voltage magnitude of all these buses has exceeded the secure state operation limit (0.9–1.1 pu). Also, it can be noticed that the voltage magnitude of bus six has dropped to zero instantaneously following the contingency. This is happening because bus six has lost its feed from the generators. A similar observation can be noticed in Fig. 7 where the frequency measurement of the buses that are directly connected to bus six

has exceeded the corresponding the secure state operation limit of 49.5–50.5 Hz after  $t=1.0$  s.

From the results of the contingency simulations, the measured data has shown that the system oscillates beyond its secure state operation limits under certain contingencies. However, the protection devices in the system may have prevented the escalation of the oscillation. For the protection of the system purposes, the benefit of a real-time DSA is clear. The method is able to provide vital information to the control center to initiate the optimized protection procedures to restore the power system operation to its secure state swiftly while minimizing the service interruption to the user.

Following the generation of the dataset for the DSA, the symmetrical uncertainty algorithm is applied to reduce the size of the dataset by removing the redundant features in the dataset. From the result, the algorithm shows a significant reduction in the total number of features. This reduction is vital to the LMT classifier performance. The training process of the classifier will be improved significantly as the dataset used for training has the minimum noise features. Additionally, since the size of the dataset has been reduced, the time required for the classifier to train in order to achieve the best performance is reduced as well.

Next, LMT classifier is applied on the reduced dataset for training and testing purposes. As described in Sect. 4, this dataset is divided into two sets of datasets; dataset for training and dataset for testing. The dataset for training consists of 70% of the reduced dataset. The remaining 30% of the reduced dataset is allocated for the testing purposes. Table 3 shows the result obtained from the application of the proposed method for DSA. The LMT classifier model shows a very high accuracy of 99.537% in assessing the dynamic security of the system. The time required to achieve this accuracy is only 0.29 s.



**Table 3** The proposed DT classifier result

Correctly classified instances in (%)	99.537
Incorrectly classified instances in (%)	0.463
The time required to build a model in (s)	0.29

**Table 4** DT classifier result with and without SU

	LMT without symmetrical uncertainty	LMT with symmetrical uncertainty
Number of features	78	9
Accuracy (%)	98.611	99.537
computational time (s)	0.39	0.29

Table 3 highlights the superiority of symmetrical uncertainty algorithms by comparing the performance of the LMT classifier build with and without the consideration of the symmetrical uncertainty in the building process. As shown in Table 4, the numbers of features in the dataset has significantly reduced from 78 to 9. This means that there are 69 redundant features or noise features in the dataset. The accuracy of the classifier increases by almost 1%. Although there is not much increment, the window for improvement in terms of the LMT accuracy of DSA application is narrow as it has achieved 98.611% accuracy even without the consideration of symmetrical uncertainty algorithm. However, the application of symmetrical uncertainty algorithm has shown significant improvement in terms of computational time in the process of building the LMT classifier model. The result shows that there is 34.483% improvement of the computational time required to build the model. These gains are very crucial especially for the real-time application as the network operators face unexpected operation changes in practice. The DSA tool needs to incorporate this new operation changes in the assessment of the dynamic security of the system. From the result, the proposed methodology may provide an elegant solution to this challenge as it is proved that it is able to build an accurate DSA classifier within a short period of time. The proposed method was tested using Intel Core i3, with 2.3 GHz CPU microprocessor.

The control center could use this vital assessment to initiate the corresponding remedial control actions to ensure that the power is kept in a secure and reliable state of operation. The results of this study have shown that the effects of cyber-attacks could be severe and could lead to blackouts if proper protection is not taken into consideration. One way to deal with a cyber-attack contingency is that the control center could directly disable the remote control for the protection relay until the encryption algorithm for the protection system has been updated. Additionally, the login credentials need

to be verified and changed frequently. The control center should reinforce the weak point that had been used by the attacker based on the protection relay log. Another useful recommendation for preventing a remote fake trip command from being sent to the protection relay is to use a confirm code from the control center to activate the remote control for the protection devices.

It should be noted that one problem with cyber-attacks is that the attacker will always try to cause significant harm to the power grid by using different ways and techniques that could give him/her the authorizing access to the grid, without leaving any digital fingerprint to the administrator. On the other hand, the primary aim of the control center is to keep the power system operate as secure as possible. Therefore, it is very difficult for the control center to consider or even imagine all possible attack scenarios in a very wide and complex system. There is no guarantee that the power grid can be 100% secure from these cyber-attackers. To develop a better defense strategy for the power grid, the control center should work based on the game theory, where a player in any game could find the Nash equilibrium when they make choices that would leave them better off, no matter what their opponents have decided to do. Therefore, this study had chosen the first defense strategy against any cyber-attack by studying the DSA. This is because the DSA could provide vital information about the security state of the power system, which can be used to create the best and fastest protection procedures to prevent the system from blackouts. The results of this study have shown the ability of this approach to be used in real-time DSA applications due to its high-speed and accuracy.

## 6 Conclusion

Assessment of the dynamic security of modern power system networks is a big challenge due to the vast number of measurements sent from numerous power network control centers. Additionally, with the massive development in cyber techniques used in the electric grid, the power system is now even more vulnerable to a new type of threat. This contingency is the cyber-attack and the impact towards the system operation is very severe. In this study, a novel method for accessing DSA that is able to deal with cyber-attack contingencies is proposed. The cyber-attack scenarios are based on the assumption that the attacker could send a fake trip command to the protection device connected to the same bus to open the CB and disconnect the corresponding transmission line. The result shows that the proposed methodology is able to classify the dynamic security of the system within a short time. Thus, this approach is suitable for the real-time DSA applications to provide crucial information for the control center to ensure the security, reliability, and continuity of

the power system operation. For future studies, more variety of scenarios are necessary to be considered in training the classifier. This is to ensure that the DSA classifier model is robust against cyber-attack.

**Acknowledgements** The authors would like to thank Universiti Tun Hussein Onn Malaysia (UTHM) for the award that enabled this research to be conducted under the Grant U424, U455 and to the Ministry of Communications (Iraq) for the technical support.

## References

- Glenn C, Sterbentz D, Wright A (2016) Cyber threat and vulnerability analysis of the us electric sector. Idaho National Lab (INL), Idaho Falls
- Zetter K (2016) Inside the cunning, unprecedented hack of Ukraine's power grid, *Wired*. Available at: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>
- Gorman S (2009) Electricity grid in US penetrated by spies, *Wall Str J* 8:A1
- Cleveland FM (2008) Cyber security issues for advanced metering infrastructure (AMI). In: 2008 IEEE power and energy society general meeting conversion and delivery of electrical energy in the 21st century, 15 p
- Rahman A, Ali M (2018) Analysis and evaluation of wireless networks by implementation of test security keys. In: International conference for emerging technologies in computing. Springer, Cham, pp 107–126
- Pan S, Morris T, Adhikari U (2015) Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Trans Ind Inf* 11:650–662
- Wang JW, Rong LL (2009) Cascade-based attack vulnerability on the US power grid. *Saf Sci* 47:1332–1336
- Sridhar S, Hahn A, Govindarasu M (2012) Cyber-physical system security for the electric power grid. *Proc IEEE* 100:210–224
- Wang J, Hui LC, Yiu S, Wang EK, Fang J (2017) A survey on cyber attacks against nonlinear state estimation in power systems of ubiquitous cities. *Pervasive Mob Comput* 39:52–64
- Liu Y, Ning P, Reiter MK (2011) False data injection attacks against state estimation in electric power grids. *ACM Trans Inf Syst Secur (TISSEC)* 14(1):13
- Hink RCB, Beaver JM, Buckner MA, Morris T, Adhikari U, Pan S (2014) Machine learning for power system disturbance and cyber-attack discrimination. In: 2014 7th international symposium on resilient control systems (ISRCs), pp 1–8
- Pan S, Morris T, Adhikari U (2015) Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Trans Smart Grid* 6:3104–3113
- Morison K, Wang L, Kundur P (2004) Power system security assessment. *IEEE Power Energ Mag* 2:30–39
- Xu L, Jiang C, Wang J, Yuan J, Ren Y (2014) Information security in big data: privacy and data mining. *Access IEEE* 2:1149–1176
- Al-Masri AN, Ab Kadir MZA, Hizam H, Mariun N (2013) A novel implementation for generator rotor angle stability prediction using an adaptive artificial neural network application for dynamic security assessment. *IEEE Trans Power Syst* 28:2516–2525
- Kucuktezcan CF, Genc VI (2012) A new dynamic security enhancement method via genetic algorithms integrated with neural network based tools. *Electr Power Syst Res* 83:1–8
- Swarup KS (2008) Artificial neural network using pattern recognition for security assessment and analysis. *Neurocomputing* 71:983–998
- Luo F, Dong Z, Chen G, Xu Y, Meng K, Chen Y et al (2015) Advanced pattern discovery-based fuzzy classification method for power system dynamic security assessment. *IEEE Trans Ind Inf* 11:416–426
- Alvarez JMG, Mercado PE (2007) A new approach for power system online DSA using distributed processing and fuzzy logic. *Electr Power Syst Res* 77:106–118
- Sun K, Likhate S, Vittal V, Kolluri VS, Mandal S (2007) An online dynamic security assessment scheme using phasor measurements and decision trees. *Power Syst IEEE Trans* 22:1935–1943
- He M, Zhang J, Vittal V (2012) A data mining framework for online dynamic security assessment: decision trees, boosting, and complexity analysis. In: Innovative smart grid technologies (ISGT), 2012 IEEE PES, pp 1–8
- He M, Vittal V, Zhang J (2013) Online dynamic security assessment with missing PMU measurements: a data mining approach. *IEEE Trans Power Syst* 28:1969–1977
- He M, Zhang J, Vittal V (2013) Robust online dynamic security assessment using adaptive ensemble decision-tree learning. *IEEE Trans Power Syst* 28:4089–4098
- Liu C, Sun K, Rather ZH, Chen Z, Bak CL, Thogersen P et al (2014) A systematic approach for dynamic security assessment and the corresponding preventive control scheme based on decision trees. *IEEE Trans Power Syst* 29:717–730
- Xu Y, Dong ZY, Zhao JH, Zhang P, Wong KP (2012) A reliable intelligent system for real-time dynamic security assessment of power systems. *IEEE Trans Power Syst* 27:1253–1263
- Al-Gubri QA, Ariff MMAM, Saeh IS (2016) Performance analysis of machine learning algorithms for power system dynamic security assessment. In: 4th IET clean energy and technology conference (CEAT 2016), 2016, pp 37–42
- Kamwa I, Grondin R, Loud L (2001) Time-varying contingency screening for dynamic security assessment using intelligent-systems techniques. *IEEE Trans Power Syst* 16:526–536
- Kamwa I, Samantaray SR, Joos G (2009) Development of rule-based classifiers for rapid stability assessment of wide-area post-disturbance records. *IEEE Trans Power Syst* 24:258–270
- Witten IH, Frank E (2005) *Data mining: practical machine learning tools and techniques*. Morgan Kaufmann, Burlington, MA, USA
- Vaiman M, Bell K, Chen Y, Chowdhury B, Dobson I, Hines P et al (2012) Risk assessment of cascading outages: methodologies and challenges. *IEEE Trans Power Syst* 27:631
- Konstantinou C, Maniatakos M (2015) Impact of firmware modification attacks on power systems field devices. *IEEE Int Conf Smart Grid Commun (SmartGridComm)* 2015:283–288
- Romeis C, Fuchs J, Jaeger J, Krebs R (2011) Innovative strategies for protection security assessment. *IEEE Power Energy Soc Gen Meet* 2011:1–6
- Romeis C, Jaeger J (2013) Dynamic protection security assessment, a technique for blackout prevention. In: *PowerTech (POWERTECH)*, 2013 IEEE grenoble, pp 1–6
- Kannan SS, Ramaraj N (2010) A novel hybrid feature selection via symmetrical uncertainty ranking based local memetic search algorithm. *Knowl Based Syst* 23:580–585
- Yu L, Liu H (2003) Feature selection for high-dimensional data: a fast correlation-based filter solution. In: *ICML*, pp 856–863
- Yu L, Liu H (2004) Efficient feature selection via analysis of relevance and redundancy. *J Mach Learn Res* 5:1205–1224
- Kaladhar D, Chandana B, Kumar PB (2011) Predicting cancer survivability using classification algorithms. *LMT* 34:96–106
- Doetsch P, Buck C, Golik P, Hoppe N, Kramp M, Laudenberg J et al (2009) Logistic model trees with AUC split criterion for the KDD cup 2009 small challenge. In: *KDD Cup*, pp 77–88
- Gupta D, Malviya A, Singh S (2012) Performance analysis of classification tree learning algorithms. *Int J Comput Appl* 55:39–44

40. Landwehr N, Hall M, Frank E (2005) Logistic model trees. *Mach Learn* 59:161–205
41. Demetriou P, Asprou M, Quiros-Tortos J, Kyriakides E (2017) Dynamic IEEE test systems for transient analysis. *IEEE Syst J* 11:2108–2117
42. Zuo C, Wang B, Zhang M, Khanwala MA, Dang S (2015) Power flow analysis using PowerWorld: a comprehensive testing report. *Int Conf Fluid Power Mechatron (FPM) 2015:997–1002*



**Qusay Al-Gburi** received his B.Sc degree in electrical engineering from the university of Mosul in 1997. He received his Master's degree in electrical and electronic engineering from University Tun Hussein Onn Malaysia (UTHM) in 2015. He worked at the Iraqi state company for Internet services (SCIS) from 2001-present. His research interests include Electrical engineer-

ing, Dynamic Security Assessment, Artificial intelligence and cyber-attack on the power system.



**Mohd Aifaa Mohd Ariff** received the B. Eng degree in electrical engineering and the M. Eng degree in electrical-power from Universiti Teknologi Malaysia (UTM) in 2008 and 2010, respectively. He received his Ph.D. degree from the Department of Electrical and Electronic Engineering, Imperial College London, London, U.K. Currently, he is a lecturer in Universiti Tun Hussein Onn Malaysia (UTHM). His current research interests include power system dynamics, coherency identifica-

tion, and adaptive system for power system protection and energy storage system.