ENHANCED DYNAMIC SECURITY ASSESSMENT FOR POWER SYSTEM UNDER NORMAL AND FAKE TRIPPING CONTINGENCIES.

qusay A. salih

A thesis submitted in fulfillment of the requirement for the award of the Doctor of Philosophy in Electrical Engineering

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

August 2019
I dedicated this thesis to my family and friends for their valuable support and encouragement during my research study and a special dedication to my uncle’s late family, who lost their lives during the attack in Mosul.
ACKNOWLEDGEMENT

First of all, gratefulness of thanks to our Creator “ALLAH” who enabled us to complete this thesis.

Special thanks go to my supervisor Dr. Mohd Aifaa bin Mohd Ariff, for having this opportunity to work under his supervision and for sharing his great knowledge and experience with me.
ABSTRACT

Recently, power system networks have become more dependent on new technologies especially in using a communication network to enhance the overall performance of system operation. The communication network facilities are applied to send and receive data and commands through the wide-area power network. However, this dependency has opened a new threat of fake tripping contingency towards the power system operation. This challenge has motivated this study to ensure that all analytical tools applied during power system operation are not affected under fake tripping contingency, especially on dynamic security assessment (DSA) classifier. To address this challenge, this study aims to investigate the impact of fake tripping contingency on the power system security via DSA classifier, then develop a novel hybrid approach for DSA classifier based on advanced feature selection technique for decision tree (DT) classifier and finally evaluate the performance of DSA classifier under normal and fake tripping contingencies, in terms of accuracy and computational time. The hybrid logistic model tree (hybrid LMT) approach proposed in this study combines the symmetrical uncertainties (SU) algorithm and the logistic model tree (LMT) algorithm. The training dataset is built by applying all possible contingencies during normal and fake tripping scenarios to the test system models. The effectiveness of the proposed approach is demonstrated on modified IEEE 9-, 14-, and 30-bus test system models due to the limitations in the simulator program. The results indicate that the hybrid LMT accurately assesses the dynamic security status of the system under normal and fake tripping contingencies with short time frame. The results show that the proposed method has 98.4126%, 98.3606%, and 99.537% accuracy and requires 22.22%, 23.529 % and 25.27% less computational time as compared to the conventional LMT algorithm in assessing the dynamic security status of the IEEE 3-machine 9-bus, the IEEE 5-machine 14-bus, and the IEEE 6-machine 30-bus test system models, respectively. In summary, the results obtained in this study offer accurate and high-speed information for the dynamic
security state, which makes DSA classifier able to provide vital information for protection and control applications to keep the power system in a secure and reliable state.
ABSTRAK

konvensional dalam menilai status keselamatan dinamik model-model sistem ujian masing-masing IEEE 3-mesin 9-bas, IEEE 5-mesin 14-bas, dan IEEE 6-mesin 30-bas. Kesimpulannya, keputusan yang diperoleh di dalam kajian ini menawarkan maklumat yang tepat dan berkelajuan tinggi untuk keadaan keselamatan dinamik yang menjadikan pengkelas DSA berupaya memberikan maklumat penting untuk perlindungan dan aplikasi kawalan demi memastikan sistem kuasa berada di dalam keadaan yang selamat dan boleh dipercayai.
## CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TITLE</td>
<td></td>
<td>i</td>
</tr>
<tr>
<td>DECLARATION</td>
<td></td>
<td>ii</td>
</tr>
<tr>
<td>DEDICATION</td>
<td></td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENT</td>
<td></td>
<td>iv</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td></td>
<td>v</td>
</tr>
<tr>
<td>ABSTRAK</td>
<td></td>
<td>vi</td>
</tr>
<tr>
<td>CONTENTS</td>
<td></td>
<td>ix</td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td></td>
<td>xiii</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td></td>
<td>xiv</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td></td>
<td>xvii</td>
</tr>
<tr>
<td>LIST OF APPENDICES</td>
<td></td>
<td>xix</td>
</tr>
</tbody>
</table>

### CHAPTER 1  INTRODUCTION

1.1 Introduction

1.2 Problem Statements

1.3 Research Objectives

1.4 Research Scope

1.5 Significant of Study

1.6 Organization of thesis

### CHAPTER 2  LITERATURE REVIEW

2.1 Introduction

2.2 Dynamic Security Assessment in Modern Power System

2.3 DSA Challenges

2.3.1 Increased Causes of Contingencies in Modern Power Systems

2.3.2 DSA Complexities
2.3.3 Non-stop Stream of Measurement Data 16
2.3.4 Fake tripping contingency 18
2.4 The Stability Criteria Addressed by DSA 22
2.5 Improving the DSA 24
2.5.1 Advanced Feature Selection 26
2.5.2 Decision Tree (DT) 29
2.6 Discussion 31
2.7 Chapter Summary 32

CHAPTER 3 METHODOLOGY 33
3.1 Overview 33
3.2 The Description of the Hybrid LMT for DSA Classifier 33
3.3 Construction of the DSA Dataset 34
3.3.1 DSA for Normal Contingency 36
3.3.2 DSA for fake tripping contingency 36
3.4 Reducing Redundant and Non-relevant Features via Feature Selection 38
3.4.1 Other Advanced Feature Selections for DSA 40
3.5 Apply DT Algorithm 42
3.5.1 Other Data Mining Algorithms for DSA 44
3.6 Chapter Summary 45

CHAPTER 4 RESULTS AND DISCUSSIONS 47
4.1 Chapter Overview 47
4.2 IEEE Test System Models 47
4.2.1 IEEE 3- synchronous machine 9-bus Test System Model 48
4.2.2 IEEE 5- synchronous machine 14-bus Test System Model 49
4.2.3 IEEE 6- synchronous machine 30-bus Test System Model 49
4.3 Application of Hybrid LMT for DSA under Normal Contingencies
   4.3.1 Application of Hybrid LMT for DSA on IEEE 3- synchronous machine 9-bus Test System Model
   4.3.2 Application of Hybrid LMT for DSA on IEEE 5- synchronous machine 14-bus Test System Model
   4.3.3 Application of Hybrid LMT for DSA on IEEE 6- synchronous machine 30-bus Test System Model

4.4 Application of Hybrid LMT for DSA on fake tripping contingency
   4.4.1 Application of Hybrid LMT for DSA on IEEE 3- synchronous machine 9-bus Test System Model
   4.4.2 Application of Hybrid LMT for DSA on IEEE 5- synchronous machine 14-bus Test System Model
   4.4.3 Application of Hybrid LMT for DSA on IEEE 6- synchronous machine 30-bus Test System Model

4.5 Performance Evaluation of the Hybrid LMT
   4.5.1 Performance Evaluation of the Hybrid LMT under Normal Contingencies
   4.5.2 Performance Evaluation of the Hybrid LMT under fake tripping Contingencies
4.6 Discussions 78
4.7 Chapter Summary 80

CHAPTER 5 CONCLUSIONS AND FUTURE RECOMMENDATIONS 81
5.1 Conclusions 81
5.2 Research Contributions 82
5.3 Future Recommendations 83

REFERENCES 84
APPENDICES 98-105
LIST OF TABLES

2.1 Issues influencing the probability of increased occurrences of contingencies 13
2.2 Applications of DSA platform 14
4.1 Performance of the hybrid LMT on IEEE 3-machine 9-bus test system model under normal contingencies 53
4.2 Performance of the hybrid LMT on IEEE 5-machine 14-bus test system model under normal contingencies 57
4.3 Performance of the hybrid LMT on IEEE 6- synchronous machine 30-bus test system model under normal contingencies 62
4.4 Performance of the hybrid LMT on IEEE 3- synchronous machine 9-bus test system model under fake tripping contingencies 65
4.5 Performance of the hybrid LMT on IEEE 5- synchronous machine 14-bus test system model under fake tripping contingencies 68
4.6 Performance of the hybrid LMT on IEEE 6- synchronous machine 30-bus test system model under fake tripping contingencies 71
4.7 Comparison of classifiers accuracy for DSA of various test system model under normal contingencies 73
4.8 Features ranks for IEEE 6- synchronous machine 30-bus test system model under normal contingencies 74
4.9 Comparison of classifiers accuracy for DSA of various test system model under fake tripping contingencies 75
4.10 Features ranks for IEEE 6- synchronous machine 30-bus test system model under fake tripping contingencies 77
## LIST OF FIGURES

1.1 Power grid infrastructure 2
1.2 The main ideas of this study 6
2.1 Causes of blackouts from 1965 to 2012 9
2.2 Secure responses for rotor angle for four generators in the IEEE-14 bus test model after a simple contingency state experiment 10
2.3 Unsecure responses for rotor angle for four generators in the IEEE-14 bus test model after a severe contingency state experiment 10
2.4 The main challenges for the DSA 12
2.5 A generic PMU 18
2.6 TCP/IP layers 21
2.7 Flowchart of generic DT structure [14] 30
3.1 Summary of the proposed research methodology 34
3.2 Dataset construction 35
3.3 Line-diagram of fake tripping contingency 37
3.4 Flowchart of feature selection processes 39
3.5 LMT classifier 44
4.1 Diagram of the modification of an existing test system models 48
4.2 Diagram of the modified IEEE 9-bus system 48
4.3 Diagram of the modified IEEE 14-bus system 49
4.4 Diagram of the modified IEEE 30-bus system 50
4.5 Generators’ rotor angle responses at (N-2 contingency scenario) 52
4.6 Voltage magnitude of all buses at (N-2 contingency scenario) 52
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7</td>
<td>Frequency of all buses connected at (N-2 contingency scenario)</td>
</tr>
<tr>
<td>4.8</td>
<td>Generators’ rotor angle responses at (N-2 contingency scenario)</td>
</tr>
<tr>
<td>4.9</td>
<td>Voltage magnitude of all buses connected to bus 2 (N-2 contingency scenario)</td>
</tr>
<tr>
<td>4.10</td>
<td>Frequency of all buses connected to bus 2 (N-2 contingency scenario)</td>
</tr>
<tr>
<td>4.11</td>
<td>Generators’ rotor angle responses at (N-1 contingency scenario)</td>
</tr>
<tr>
<td>4.12</td>
<td>Voltage magnitude of all buses connected to bus 2 at (N-1 contingency scenario)</td>
</tr>
<tr>
<td>4.13</td>
<td>Frequency of all buses connected to bus 2 (N-1 contingency scenario)</td>
</tr>
<tr>
<td>4.14</td>
<td>Generators’ rotor angle responses at (N-2 contingency scenario)</td>
</tr>
<tr>
<td>4.15</td>
<td>Voltage magnitude of all buses connected to bus 2 at (N-2 contingency scenario)</td>
</tr>
<tr>
<td>4.16</td>
<td>Frequency of all buses connected to bus 2 (N-2 contingency scenario)</td>
</tr>
<tr>
<td>4.17</td>
<td>Generators’ rotor angle responses for server fake tripping contingency on bus 4</td>
</tr>
<tr>
<td>4.18</td>
<td>Bus voltage responses for server fake tripping contingency scenario on bus 4</td>
</tr>
<tr>
<td>4.19</td>
<td>Frequency responses for server fake tripping contingency scenario on bus 4</td>
</tr>
<tr>
<td>4.20</td>
<td>Generators’ rotor angle responses at fake tripping contingency on bus 2</td>
</tr>
<tr>
<td>4.21</td>
<td>Bus voltage responses for server fake tripping contingency scenario on bus 2</td>
</tr>
<tr>
<td>4.22</td>
<td>Frequency responses for server fake tripping contingency scenario on bus 2</td>
</tr>
<tr>
<td>4.23</td>
<td>Generators’ rotor angle responses at fake tripping contingency on 6</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>4.24</td>
<td>Bus voltage responses for server fake tripping contingency scenario on bus 6</td>
</tr>
<tr>
<td>4.25</td>
<td>Frequency responses for server fake tripping contingency scenario on bus 6</td>
</tr>
</tbody>
</table>
# LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA</td>
<td>Dynamic Security Assessment</td>
</tr>
<tr>
<td>DT</td>
<td>Decision Tree</td>
</tr>
<tr>
<td>EPRI</td>
<td>Electric Power Research Institute</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>LMT</td>
<td>Logistic Model Tree</td>
</tr>
<tr>
<td>NERC</td>
<td>North American Electric Reliability Council</td>
</tr>
<tr>
<td>PJM</td>
<td>Interconnection power system in the United States of America</td>
</tr>
<tr>
<td>PMU</td>
<td>Phasor Measurement Units</td>
</tr>
<tr>
<td>Rated kV</td>
<td>Machine-rated terminal voltage in kV; base kV for impedances</td>
</tr>
<tr>
<td>Rated MVA</td>
<td>Machine-rated MVA; base MVA for impedances</td>
</tr>
<tr>
<td>SU</td>
<td>Symmetrical uncertainty</td>
</tr>
<tr>
<td>D</td>
<td>Machine load damping coefficient</td>
</tr>
<tr>
<td>$E_1$</td>
<td>Field voltage value, 1 in p.u.</td>
</tr>
<tr>
<td>$E_2$</td>
<td>Field voltage value, 2 in p.u.</td>
</tr>
<tr>
<td>$F$</td>
<td>Shaft output ahead of reheater in p.u.</td>
</tr>
<tr>
<td>$H(s)$</td>
<td>Inertia constant in s</td>
</tr>
<tr>
<td>$K_a$</td>
<td>Regulator gain (continuous acting regulator) in p.u.</td>
</tr>
<tr>
<td>$K_e$</td>
<td>Exciter self-excitation at full load field voltage in p.u.</td>
</tr>
<tr>
<td>$K_f$</td>
<td>Regulator stabilizer circuit gain in p.u.</td>
</tr>
<tr>
<td>$P_{max}$</td>
<td>Maximum turbine output in p.u.</td>
</tr>
<tr>
<td>$R$</td>
<td>Turbine steady-state regulation setting or droop in p.u.</td>
</tr>
<tr>
<td>$S(1.0)$</td>
<td>Machine saturation at 1.0 p.u. voltage in p.u.</td>
</tr>
<tr>
<td>$S(1.2)$</td>
<td>Machine saturation at 1.2 p.u. voltage in p.u.</td>
</tr>
<tr>
<td>$S_{E(E1)}$</td>
<td>Saturation factor at E1</td>
</tr>
<tr>
<td>$S_{E(E2)}$</td>
<td>Saturation factor at E2</td>
</tr>
<tr>
<td>$T''_{d0}$</td>
<td>d axis subtransient open circuit time constant in s</td>
</tr>
<tr>
<td>$T''_{q0}$</td>
<td>q axis subtransient open circuit time constant in s</td>
</tr>
</tbody>
</table>
\( T'_{d0} \) - d axis transient open circuit time constant in s

\( T'_{q0} \) - q axis transient open circuit time constant in s

\( T_1 \) - Control time constant (governor delay) in second

\( T_2 \) - Hydro reset time constant in second

\( T_3 \) - Servo time constant in second

\( T_4 \) - Steam valve bowl time constant in second

\( T_5 \) - Steam reheat time constant in second

\( T_a \) - Regulator time constant in second

\( T_e \) - Exciter time constant in second

\( T_f \) - Regulator stabilizing circuit time constant in second

\( T_r \) - Regulator input filter time constant in second

\( V_{R\text{max}} \) - Maximum regulator output, starting at full load field voltage in p.u.

\( V_{R\text{min}} \) - Minimum regulator output, starting at full load field voltage in p.u.

\( r_a \) - Armature resistance in p.u.

\( x''_{d} \) - Unsaturated d axis subtransient reactance in p.u.

\( x''_{q} \) - Unsaturated q axis subtransient reactance in p.u.

\( x'_{d} \) - Unsaturated d axis transient reactance in p.u.

\( x'_{q} \) - Unsaturated q axis transient reactance in p.u.

\( x_{d} \) - Unsaturated d axis synchronous reactance in p.u.

\( x_{l} \text{ or } x_{p} \) - Leakage or Potier reactance in p.u.

\( x_{q} \) - Unsaturated q axis synchronous reactance in p.u.
## LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Vita</td>
<td>98</td>
</tr>
<tr>
<td>B</td>
<td>List of Publication</td>
<td>99</td>
</tr>
<tr>
<td>C</td>
<td>IEEE 9-Bus Modified Test System Data</td>
<td>99</td>
</tr>
<tr>
<td>D</td>
<td>IEEE 14-Bus Modified Test System Data</td>
<td>103</td>
</tr>
<tr>
<td>E</td>
<td>IEEE 30 Bus Modified Test System Data</td>
<td>105</td>
</tr>
<tr>
<td>F</td>
<td>Some of the Screenshots for Study Programs</td>
<td>105</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

The electric power system network is the backbone of energy in any country. It is responsible for transmitting power to the customers from the generation side through a wide and complex network that includes a huge number of devices and equipment. In general, this network contains two crucial layers. The first layer is responsible for facilitating electricity flows from the utility to the customer. This layer is divided into three main sections, namely, generation, transmission, and distribution. The second layer is responsible for facilitating communication for power system operation. This layer sends control commands and receives information from the power carry layer to the control center. Figure 1.1 shows the general layers in a power grid infrastructure.

The communication network layer includes different media, such as telephone lines, microwaves, satellites, and fiber optics. The communication network offers many advantages for the control center operation, while simultaneously reducing the operation cost for the power system. Therefore, electrical utilities have made various efforts to develop this vital network and its operation. However, a communication network is prone to failures due to different reasons, which include human error, malfunctioning of equipment, and limitations of the communication architecture and cyber-attack. Based on a report by the North American Electric Reliability Council (NERC), failures in communication and information system is the root cause of 32% of power outages [2]. For example, one of the reasons for the North America blackout in 2003 was a computer system’s failure that send an
unwanted alarm signal to the control center [3]. Therefore, communication failures have a significant impact on power system operation.

![Power Grid Infrastructure Image](image.png)

**Figure 1.1: Power grid infrastructure [1]**

The high integration of communication technology into the power grid which uses a weak secured communication protocol in sending and receiving data and commands through wide power network makes it more vulnerable to the new threat to the power grid that is fake tripping. Where fake tripping could trigger the circuit breaker (open/close) and cause a fake tripping contingency on the power system. One off fake tripping is cyber-attack [4]. Based on Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector report, cyber-attack is “an attempt to infiltrate information technology systems, computer networks, or individual computers with a malicious intent to steal information, cause damage, or destroy specific targets within the system” [5]. The impact of a cyber-attack in the power system could be devastating for electric companies and users. This is for the ability of the attacker to make a direct impact on the power transmission operation. The cyber-attack could access the communication network via various technical channels where an attacker could exploit the weaknesses in protection procedures or the weaknesses in data encryption sent over the wide network.
In general, a cyber-attack in the power system can be classified into two types: individual and non-individual. The individual attack is simpler between these two attacks where the target of this one is to change the consumed power by the users by hacking the smart electric meter to reduce the cost of electricity bills [6]. While, the non-individual attack is the dangerous attack aiming to cut off the electrical service by trying to access the generators, control or protection devices or control for the drop load. This kind of attack is usually based on 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 [7].

It is worth noting that the main concern with cyber-attacks is that: the attacker will always try to cause major harm to the power grid by using different ways and techniques that could give them the authorizing access to the grid, without leaving any "fingerprints" if possible (e.g., there are various ways and channels for these attackers to gain access to the network). Meanwhile, the main target of the control center is to keep the power system secure by using traditional techniques and training. Thus, each one has a different perspective and training. Therefore, it is very challenging for the network operator to consider or estimate all possible attack scenarios in a very wide and complex system. There is no guarantee that the power grid can be 100% secured from cyber-attacks since the game between an attacker and a control center is a dynamic game. To develop a better defense strategy for the power grid, the control center should follow an optimization approach for example using Game Theory [8] to reach a strategy where the system has no incentive to change its strategy (Nash Equilibrium), taking into account normal and cyber-attack contingencies as cost functions in the optimization design. Definitely, this kind of defense strategy could not prevent cyber-attacker, but it is able to help system operator to mitigate the server of cyber-attack contingency and prevent the blackout.

In order to keep the power system in a reliable and secure state, control centers should evaluate the security of the system following contingencies via a dynamic security assessment (DSA) tool. The DSA is an essential tool for monitoring and of assessing the state of security of the power system’s behaviors (meaning secure or insecure) after a contingency has occurred. Therefore, studying the impact of contingency that is caused by fake tripping towards DSA is very important for the control center to improve network response against this kind of attack.
Traditionally, DSA includes multiple-algebra equations that could consume a long time to solve. Moreover, the study of DSA based on the normal contingencies that arises from lightning, normal failure of the protection devices, and overload. Recently, with the continued growth in the size of power networks, which is accompanied by implementation of many new technologies (e.g. as Phasor Measurement Units, smart grids and smart meters) that have helped to provide a snapshot for system state and at the same time leads to an increase in the data that needs to be processed when the contingency occurs. Additionally, with the increased probability of exposure to cyber-attacks on the power grid, the control center should develop a DSA tool that meets the needs for assessing dynamic security state with accurate result and a short time frame [9-12] and develop a better defense strategy to protect the power system against new threats that are fake tripping related and include it in simulations and analyses of the DSA tool.

In this study, a new approach has been developed for DSA tool to deal with online DSA challenges also to represent and analyze the effect of "fake tripping contingency" on the power system security via DSA tool. The target was to build an accurate and high-speed classifier. Thus the control center could trigger the accurate protection procedures to protect the power system where wrong protection steps could result in a high cost for the system operator.

1.2 Problem Statements

The power system network is one of the most complex human-made set-ups in the world. This network includes very large transmission line equipment that are installed in a sprawling geographical area which has different operation and environment factors. Security for power system is a crucial aspect, it prevents the occurrence of a blackout. Recently, the power system has witnessed many blackouts due to different types of contingencies affecting millions of people.

To ensure a continuous work of the power system network, control center must keep it in a secure state following contingencies to prevent blackout occurrence, DSA tool is used to evaluate the ability of the power system to withstand sudden disturbances and to survive the transition to an acceptable steady state. Then based
on the assessment for DSA, the operator could activate an accurate and fast protection processes to protect the network.

Based on the reviewed papers in this study, the new operating environment for power system made the DSA tool facing many challenges such as increased number of contingencies, a huge amount of measurement data stream from different network devices, which should be processed within a short time frame. Moreover, because the network is depending on the new weakly protected communication technology, a new threat to the power network which is originating from severe fake tripping contingency has appeared. This kind of contingency could be severe on the power security state due to the limitations of traditional defense and analysis strategies for the control center to deal with this kind of recent contingency.

There are several reported attempts to improve the DSA tools application in the literature such as the use of traditional time-domain simulation or data mining technologies. These approaches used the conventional DSA which is developed based on normal contingency evaluations only and this security criterion for power network operation is inadequate to address fake tripping contingency events. Despite the mentioned attempts, it remains a challenging task for the DSA tool in the present and future requirements to evaluate security system state due to the DSA computational complexity that is incurred by the massive scale data of the power network which increases every year and the large list of the contingencies.

Therefore, a new approach should be adopted to improve DSA classifier towards these recent and future challenges by trying to study the effect of a new threat of fake tripping contingency on power grid security state. Moreover, finding technical ways to reduce the stream dataset features in an effective way to enhance the result in terms of accuracy along with speed. The target is to build a robust DSA classifier that could be used to provide vital information for protection and control applications in power system operation to keep the network in a secure state and prevent the occurrence of blackouts.

Figure 1.2 briefly shows the research problem, its challenge, and the proposed solution.
1.3 Research Objectives

This research aims to achieve the following objectives:

i) To study the effects of fake tripping contingencies on the power system security via DSA.

ii) To develop a novel hybrid approach for DSA classifier based on advanced feature selection technique for decision tree (DT) classifier.

iii) To evaluate the performance of DSA classifier under normal and fake tripping contingencies, in terms of accuracy and computational time.

1.4 Research Scope

This research is limited to the following scope:

i) The simulators of the power system respond to normal and fake tripping contingencies for dynamic security assessment are carried out on the PowerWorld simulator platform.

ii) Symmetrical uncertainty (SU) is considered as a feature selection algorithm to reduce the redundant and irrelevant features in the dataset.

iii) Logistic Model Tree (LMT) is considered as the decision tree algorithm to develop the classifier model for the DSA.

iv) Waikato Environment for Knowledge Analysis (WEKA) program was used for implementing data mining technology.

v) The proposed algorithm is evaluated on the modified IEEE 9-bus, 14-bus, and 30-bus benchmark test systems model.
REFERENCES


Symmetrical Uncertainty Ranking Based Local Memetic Search Algorithm.

110. Yu, L. and Liu, H. Efficient Feature Selection via Analysis of Relevance and

111. Kaladhar, D. S., Chandana, B. and Kumar, P. B. Predicting Cancer

112. Ruiz, R., Riquelme, J. C. and Aguilar-Ruiz, J. S. Incremental Wrapper-Based
Gene Selection from Microarray Data for Cancer Classification. Pattern

113. Kumar, A. and Zhang, D. Personal Recognition Using Hand Shape and


115. Demetriou, P., Asprou, M., Quiros-Tortos, J. and Kyriakides, E. Dynamic

116. Hutcheon, N. and Bialek, J. W. Updated and Validated Power Flow Model of
the Main Continental European Transmission Network. 2013 IEEE Grenoble


118. Chen, Jingnian, Houkuan Huang, Fengzhan Tian, and Shengfeng Tian. A
Selective Bayes Classifier for Classifying Incomplete Data Based on Gain

119. Günel, Serkan. Hybrid Feature Selection for Text Classification. Turkish
Journal of Electrical Engineering & Computer Sciences 20, 2012, Sup. 2:
1296-1311.

120. Huang, Yue, Paul J. McCullagh, and Norman D. Black. An Optimization of
Relief for Classification in Large Datasets. Data & Knowledge Engineering
68, 2009, 11: 1348-1356H

121. Elomaa, Tapio, and Matti Kaariainen. An Analysis of Reduced Error Pruning.

of Western Himalayan Indian State of Himachal Pradesh Using J48

