8-14-2015

Event and Intrusion Detection Systems for Cyber-Physical Power Systems

Uttam Adhikari

Event and intrusion detection systems for cyber-physical power systems

By

Uttam Adhikari

A Dissertation
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in Electrical and Computer Engineering
in the Department of Electrical and Computer Engineering

Mississippi State, Mississippi

August 2015

Event and intrusion detection systems for cyber-physical power systems

By

Uttam Adhikari

Approved:

_____

Thomas H. Morris
(Major Professor)

_____

Roger L. King
(Committee Member)

_____

Yong Fu
(Committee Member)

_____

Robert Wesley McGrew
(Committee Member)

_____

James Fowler
(Graduate Coordinator)

_____

Jason M. Keith
Dean
Bagley College of Engineering

Name: Uttam Adhikari

Date of Degree: August 14, 2015

Institution: Mississippi State University

Major Field: Electrical and Computer Engineering

Major Professor: Dr. Thomas H. Morris

Title of Study: Event and intrusion detection systems for cyber-physical power systems

Pages in Study: 188

Candidate for Degree of Doctor of Philosophy

High speed data from Wide Area Measurement Systems (WAMS) with Phasor Measurement Units (PMU) enables real and non-real time monitoring and control of power systems. The information and communication infrastructure used in WAMS efficiently transports information but introduces cyber security vulnerabilities. Adversaries may exploit such vulnerabilities to create cyber-attacks against the electric power grid. Control centers need to be updated to be resilient not only to well-known power system contingencies but also to cyber-attacks. Therefore, a combined event and intrusion detection systems (EIDS) is required that can provide precise classification for optimal response.

This dissertation describes a WAMS cyber-physical power system test bed that was developed to generate datasets and perform cyber-physical power system research related to cyber-physical system vulnerabilities, cyber-attack impact studies, and machine learning algorithms for EIDS. The test bed integrates WAMS components with a Real Time Digital Simulator (RTDS) with hardware in the loop (HIL) and includes various

sized power systems with a wide variety of implemented power system and cyber-attack scenarios.

This work developed a novel data processing and compression method to address the WAMS big data problem. The State Tracking and Extraction Method (STEM) tracks system states from measurements and creates a compressed sequence of states for each observed scenario. Experiments showed STEM reduces data size significantly without losing key event information in the dataset that is useful to train EIDS and classify events.

Two EIDS are proposed and evaluated in this dissertation. Non-Nested Generalized Exemplars (NNGE) is a rule based classifier that creates rules in the form of hyperrectangles to classify events. NNGE uses rule generalization to create a model that has high accuracy and fast classification time. Hoeffding adaptive trees (HAT) is a decision tree classifier and uses incremental learning which is suitable for data stream mining. HAT creates decision trees on the fly from limited number of instances, uses low memory, has fast evaluation time, and adapts to concept changes. The experiments showed NNGE and HAT with STEM make effective EIDS that have high classification accuracy, low false positives, low memory usage, and fast classification times.

DEDICATION

To my wife Poornima, Dad Sitaram, Mom Sita, Grand Dad Danda Pani, Grand Mom Chhaya Devi, Brothers Ashok and Kanchan

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my advisor, Dr. Thomas Morris, for his excellent guidance, care, and for patiently correcting my writing. I am grateful to him for financially supporting my research and for making me a better person both academically and personally by providing advices beyond textbooks and research.

I would like to express my gratitude to Dr. Roger King for giving me opportunity to be involved in this research work and for constant guidance throughout the research work. I would like to acknowledge Dr. Yong Fu and Dr. Wesley McGrew for their advice and support as members of my graduate committee.

I would like to thank Shengyi Pan, who as a good companion, was always willing to help and give his best suggestions and help me provide insights into the cyber security issues in power systems.

I would like to thank Mississippi State University, ECE Department, Starkville community, Starkville Nepalese community, my friends, and relatives for their support.

I would also like to thank my parents for their unconditional love who instilled regard for higher education and taught me to inherit culture of giving back. I would like to thank my two brothers Ashok and Kanchan who were always supporting me. I would also like to thank Suryama for painstakingly correcting my writing.

Finally, I would like to thank my wife, Poornima. She has been a true and great supporter during my good and bad times. I would like to thank her for unconditional love, sacrifices, and for being instrumental in instilling my confidence.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Background

The fundamental principle of power system operation is to maintain balance between generation and load demand in order to safely operate the system within acceptable stability and reliability limits. Due to increasing electricity demand and inadequate expansion of grid infrastructure, operators are forced to operate the power system close to the stability limit. The integration of renewable energy sources, deregulation, and multipoint communication between consumers and utilities has introduced more complexities that make power system operation very difficult to manage. The traditional preventive controls based on a predefined set of credible contingencies may not be sufficient due to changing operating conditions. Hence, appropriate real time situational awareness and corrective action is required to prevent any unstable condition which could cause catastrophe [1].

From past experiences of large blackouts, it is evident that these events evolve and propagate faster than the sector's current ability to detect such events and respond with counter measures. It is also known that large black outs start from single or multiple contingencies due to overloading, faults, and scheduled and emergency outages. One of the contributing factors in many power system failures is the lack of ability to visualize the real time state of the electric grid. Poor visibility across the power system may cause

the operators to take incorrect control actions which in turn may lead to power system black outs [1]. Also, coordinated cyber-attacks may create N-k contingencies and cause cascading failures over large areas of operation. These attacks against power systems are not a myth but are credible threats as evidenced from attacks against industrial control systems in other critical infrastructure categories [2]. Due to the scale of impact areas, large outages can have tremendous socio-economic impact. For example, the economic impact due to the North American blackouts in 2003 was more than 10 billion US dollars [3].

Due to the nature of deregulated and interconnected systems spread over large geographical areas, and inefficient information exchange mechanisms between the neighboring utilities and Independent System Operators (ISO) or Regional Transmission Operators (RTO), proper system visibility is lacking. The slow sample rate of SCADA systems does not capture system dynamics properly, and, hence cannot provide true states of the systems in real time [1]. These key inadequacies are seen as one of the major factors in poor situational awareness in the control center. Wide Area Measurement Systems (WAMS) are based on synchrophasor measurements and were developed to address these inadequacies. A Phasor measurement synchronized with Universal Time Coordinated (UTC) time is called a synchrophasor. Significant efforts are being made to deploy WAMS across the world. WAMS consists of Phasor Measurement Units (PMU) and Phasor Data Concentrators (PDC) connected with high speed communication networks as shown in Figure 1.1. WAMS are heavily based on information technology (IT) infrastructure and communication takes place between various devices and entities that use many different protocols. The PMU is a fundamental component of WAMS and

has brought a paradigm shift in monitoring and control of power systems because of its time synchronized high speed data streaming capabilities up to 120 samples per second with 1 microsecond time accuracy.

1.2 Motivation

The granularity of Synchrophasor data obtained from a PMU is very high. PMU sample rates provide greater visibility of power system events and enable the capture system dynamic details which were impossible before [1]. The applications of Synchrophasor technology focus on improving system monitoring and visualization for an operator's improved situational awareness, enhancing the utilization of existing grid resources through efficient management, providing enhanced post event forensic analysis, and providing better tools to validate and estimate system parameters [4]. WAMS provide near real time monitoring and visualization capability of a grid, oscillation monitoring, frequency monitoring, voltage stability monitoring, event detection, and power system state estimation. WAMS is also useful for islanding detection and restoration as well as transmission congestion management [4].

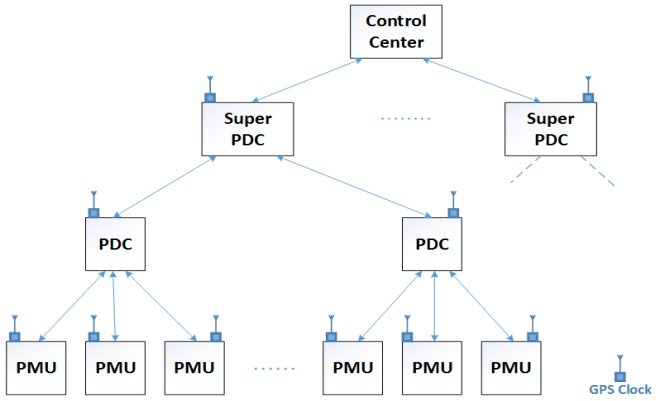


Figure 1.1 Wide Area Measurement Systems (WAMS)

The measurements obtained from power system WAMS are essential for evaluating and developing new algorithms and tools for power system operations. However, data associated with power system scenarios are difficult to obtain, especially when scenarios are very rare, such as larger black outs, complex cascading failures, and scenarios related to cyber-attacks. It is impractical to wait for such events to happen. Utilities can be a good source of such data. However, these data are often confidential and proprietary in nature, do not include all possible scenarios, and, are also difficult to understand. Researchers typically have to sign a strict non-disclosure agreement (NDA) to obtain data. Data unavailability is a significant challenge to the power energy society machine learning research community [5] [6]. Hence, an alternative data generation method is required. This data scarcity motivated us to create a WAMS test bed so that researchers can have datasets according to their requirements with greater flexibility in the scenarios.

Since, WAMS use high speed communication networks, more efficient monitoring and control is possible. However, the integration of software applications, hardware, communication networks, and protocols introduce many vulnerabilities that could be potential insertion points for exploits. These vulnerabilities, if not addressed before deploying in the field, could bring catastrophic grid failure due to cyber-physical attacks. Attacks on control system confidentiality, integrity and availability are a prime concern. WAMS components may be targeted with different attacks. Malicious command injection and switching attacks [7] [8], denial of service (DoS) attacks, attacks against open ports and services, device access hijacking, man in the middle (MITM) attacks [9] [10], device setting changes, and attacks on HMI are some of the potential cyber-attacks

against bulk power systems [11]. An attack against Iranian nuclear centrifuges is one of the many examples of a cyber-attack in which an attacker injected malware to modify control system behavior [2]. Power system cyber security has been overlooked in the past and has not been addressed adequately as cyber-attacks were not considered a major threat. The WAMS security concern motivated us to create a cyber-physical test bed which is capable of providing a platform for vulnerability assessment, attack modeling, and impact analysis.

The dawn of the WAMS created significant buzz among the power utilities, ISOs, RTOs, power system experts, and researchers. Due to an abundance of the information provided by WAMS, new methods of analyzing system events and development of data driven tools are emerging. Traditional complex mathematical solution based tools can be complemented by the use of new machine learning based data mining techniques. The traditional batch processing data mining methods and data stream mining techniques can be used to extract useful information from a huge volume of data. These methods bring an opportunity to provide faster and better tools in the control center. Machine learning, data mining, also known as knowledge discovery from data (KDD), and pattern discovery techniques are suitable to learn and extract information from these 'Big Data' sets as defined by volume, velocity, and variety [12]. The sequence of events and patterns in heterogeneous datasets are key characteristics that can be used to discriminate natural events and cyber intrusions. Decision rules and trees obtained from classification and regression are important components of advanced situational awareness tools in real and non-real time. These methods can be used to develop effective event and intrusion detection systems (EIDS). However, the size of the data provided by WAMS poses

significant challenges on data management and storage. Also, most traditional machine learning algorithms are designed to work with limited datasets. This limitation motivated us to explore new ways of data size reduction and compression techniques, and examine the efficacy of datasets by evaluating the performance of machine learning and data mining algorithms.

In summary, WAMS have tremendous advantages, reliable tools are still not fully deployable and require more research and development work to ensure the efficacy of the tools and security of WAMS. However, current research on cyber-physical security of WAMS and data mining is constrained by a lack of proper cyber-physical test beds that realistically represent the power system during normal and abnormal conditions, provide real time hardware in the loop (HIL) simulation, and incorporate a large number of scenarios. Additionally, lack of a test bed for vulnerability assessment of synchrophasor based WAMS, proper modeling of cyber-physical attacks against power systems and impact analysis, and lack of big datasets that are essential for testing machine learning based data mining techniques motivated us to develop the WAMS cyber-physical test bed and heterogeneous datasets required for power system engineers, cyber-security researchers, and data scientists.

1.3 Objective

1.3.1 Objective 1

This work addresses constraints mentioned in the previous section. The *first* objective of the research work is to develop a WAMS cyber-physical test bed that facilitates a platform for real time simulation of power system and event analysis, relay testing and validation, wide area protection algorithm testing and validation, dataset and

application development, cyber-physical attack modeling and simulation, cyber-attack impact analysis and mitigation strategy development, vulnerability assessment and penetration testing, interoperability studies, digital forensic analysis, and EIDS development. This test bed enables a collaboration of cross disciplinary research from power system, cyber security, and data science. It is hypothesized that a real time digital simulator (RTDS) can be used to develop a WAMS based cyber-physical test bed in hardware in the loop (HIL) simulation which provides an excellent platform for integrating hardware relays, PMU, PDC, IT infrastructures, communication network protocols, and other I/O devices to create realistic WAMS in the laboratory environment. The WAMS architecture can be implemented to achieve the above mentioned goals.

1.3.2 **Objective** 2

The WAMS provides various information related to power system operation. The PMU provides voltage and current phasors, frequency, rate of change of frequency, sequence components, and other digital status information. Similarly, other components such as relays, control center computers, Snort engines, and other custom calculated information can be used in EIDS. As mentioned earlier, power system engineers, cyber security researchers, and data scientists working on data mining techniques require high volumes of data. The datasets should be random enough to test the performance of data mining algorithms. In addition to that, the test bed should be able to create a "Big Data" sets without human supervision. The *second* objective of this work is to create heterogeneous datasets that represent the various power system events such as faults, outages, and cyber-physical attacks. The datasets are created by integrating data from PMUs, relays, Energy Management Systems (EMS) logs, network transaction

information obtained from Snort logs, and other custom calculations. It is hypothesized that RTDS, MATLAB, Python script, AUTOIT scripts, PDC, PDC software, and OpenPDC can be used to automate the simulation, simulate attacks, randomize the scenarios with random fault locations and random load conditions, and finally integrate the data generated during the simulation. These datasets are critical to power system event detection, intrusion detection systems (IDS), EIDS, data stream mining, and machine learning methods for power systems.

1.3.3 Objective 3

The data management and processing is a challenging research area. WAMS generate a very high volume of data. A significant amount of data is redundant information. Proper data integration, cleaning, and transformation without losing information enables efficient algorithms development and testing. Many traditional batch processing methods in machine learning algorithms load the data into memory and then process it. If the data is too large it is impossible to load and process the data. The *third* objective of the work is to develop a novel method to transform data that is suitable for developing EIDS using sequential data mining techniques as well as to evaluate machine learning and data stream mining algorithms. It is hypothesized that the state tracking and extraction method (STEM) can be used to quantize and compress the heterogeneous datasets to reduce the size of data while preserving original key events and patterns within the datasets, and automate the EIDS rule generation for large number of scenarios.

1.3.4 **Objective** 4

A large problem in power system cyber-security is that the systems are not resilient to cyber-attacks. For decades power systems are designed to be resilient to contingencies. Cyber-attacks are a new cause of contingencies and power system control systems need to be updated to be resilient not only to previously known contingencies but to cyber-attacks as well. A combined event detector that can provide a precise classification of all types of contingencies is needed to enable algorithms to automate responses. Resilience requires first identifying the ongoing contingency and then executing a valid response. So, an event and intrusion detection systems (EIDS) must be able to classify a wide variety of scenarios with high accuracy, have low memory usage to enable scaling, and have classification times faster than synchrophasor data reporting times to enable faster response.

Decision trees [13] [14], support vector machines [15] [16], and artificial neural networks [17] [18] have been used in various power system application studies. Traditional machine learning algorithms can be used in event classification and intrusion detection. Traditional machine learning algorithms are designed to work with small volumes of data and are sensitive to memory limitations. Hence, the data requires significant further processing to address this limitation. The *fourth* objective of this work is to develop an EIDS using a traditional batch processing machine learning algorithm with very high accuracy over wide range of scenarios, which handles large volume and velocity WAMS data, and has fast classification time. The hypothesis of this work is that nearest neighbor-like Non-Nested generalized exemplars (NNGE) algorithm with STEM

data processing technique is suitable to create an effective EIDS that fulfils these requirements. The results from experiments support this hypothesis.

1.3.5 **Objective** 5

One important advantage of WAMS is real time event reporting. Traditional machine learning requires training to build a model. Real time classification methods must adapt to changing conditions of the power system. Hence, incremental learning methods are required. Incremental learning methods address the memory issue that limit traditional batch processing methods scalability. Data stream mining techniques have been previously evaluated for power system event detection. Data stream mining takes the dynamic behavior of power systems into account by learning concepts from evolving data streams [19]. The *fifth* objective of this work is to develop a real time EIDS that uses stream data mining. The stream data mining EIDS will handle large datasets, with very high quality and accurate classification, have a small memory footprint, and have faster evaluation time than the current synchrophasor data rate. The hypothesis of this work is that the drift detection method (DDM) with Hoeffding Adaptive Trees (HAT) and adaptive windowing (ADWIN), hence HAT, can be used for data stream mining to create an EIDS for real time application which meets the aforementioned requirements. Evaluation of the HAT EIDS was performed by measuring accuracy of the classification, kappa statistic, evaluation time, and RAM-hours. The results from experiments support this hypothesis.

1.4 Contributions

This work has 5 significant contributions which together provide a means for securing cyber physical power systems.

1. A one of kind of WAMS based cyber physical test bed was developed with hardware in the loop simulation capability which provides a platform for power system engineers, cyber security researchers, and data scientist to evaluate the physical and network related artifacts of power system contingencies and cyber-attacks.
2. Power system, cyber security, and data science researchers are starved for useful data which enables research. Heterogeneous datasets were created and shared with researchers for power system event detection, dimension reduction, data stream mining, EIDS, and machine learning methods for cyber-power event (a combination of cyber-attacks and power system events) detection.
3. Approaches are needed to support efficient consumption of high velocity and high volume WAMS data in conjunction with data from other asynchronous sources. The STEM algorithm was developed to transform, compress, and reduce the size of the heterogeneous WAMS data while maintaining key patterns in the data to enable machine learning based classification. STEM provides compression ratio of up to 4178 to 1. STEM was successfully used with common path mining, NNGE, and HAT classifiers.

4. NNGE with STEM preprocessing was evaluated and shown to provide effective event and intrusion detection by leveraging high velocity and high volume heterogeneous WAMS data and providing precise classification of cyber-power events. The EIDS was evaluated using data sets with 12 power system contingencies and 33 cyber-attacks. The resulting EIDS performance benchmarks include 95% classification accuracy for binary and 93% for multiclass, less than 5% and 1.5% false positive rate for binary and multiclass respectively, and less than 0.3 millisecond classification time.
5. HAT with STEM preprocessing was evaluated and shown to provide effective event and intrusion detection with real time classification and continuous incremental learning. HAT with STEM preprocessing was evaluated using data sets with 12 power system contingencies and 33 cyber-attacks. HAT benchmarks include over 96% classification accuracy for binary and 92% classification accuracy for multiclass, less than 9×10^{-7} average RAM-hours memory, and less than 0.1 millisecond evaluation time per instance.

1.5 Dissertation outline

This dissertation is organized as follows:

- Chapter I: This chapter introduces problems and provides a brief background on power system operation. It also discusses the motivation of the research and provides specific objectives of the research. It summarizes the contributions of the research work.

- Chapter II: This chapter describes the WAMS test bed architecture, test bed scenarios and examples, and test bed applications in power system and cyber security domain. It also provides a dataset development process with some example datasets.
- Chapter III: This chapter presents State Tracking and Extraction Method (STEM) for high volume WAMS heterogeneous data processing for cyber-physical power systems. Also, it presents results on patterns and data size reduction at different steps of STEM.
- Chapter IV: This chapter presents the nearest neighbor like non-nested generalized exemplar (NNGE) algorithm. The implementation of NNGE to develop an effective EIDS for cyber-physical power system is discussed in this chapter. Several experiments to evaluate the performance of NNGE for EIDS and results are presented.
- Chapter V: This chapter presents a real time EIDS which uses the Hoeffding Adaptive Tree (HAT) algorithm for data stream mining. HAT to develop real time EIDS for cyber-physical power system is discussed. Several experiments are presented to evaluate the suitability of HAT for real time EIDS and results are presented.
- Chapter VI: This chapter is conclusion and discussion of future works. This chapter summarizes the methods and results obtained from various research work presented in this dissertation and possible future work to extend.

CHAPTER II

DEVELOPMENT OF WAMS CYBER-PHYSICAL TEST BED FOR POWER SYSTEM, CYBER SECURITY, AND DATA MINING

2.1 Introduction

Researchers from various cross disciplinary fields such as power system, data science, and cyber-power security working on synchrophasor based wide area measurement systems (WAMS) are facing two distinct challenges. First, the lack of a comprehensive test bed that integrates physical power systems with industry grade hardware, software, and WAMS standard protocols impedes the study of cyber security issues and vulnerabilities related to WAMS hardware, software, communication protocols, and consequences of exploitation of such vulnerabilities in power system operation. Second, the lack of appropriate synchrophasor data along with other information imposes challenges to develop and evaluate applications based on heterogeneous datasets using data mining algorithms. In this work, as a first contribution, a WAMS cyber-physical test bed with hardware in the loop (HIL) is developed by integrating physical power system emulated in RTDS, communication networks and protocols, control and monitoring devices, and software. The WAMS cyber-physical system integrates industry standard WAMS hardware, software, communication networks, and protocols. As second contribution, an automated simulation and control engine to randomize various cyber-physical power system events, and create large

heterogeneous datasets without human supervision is developed. The WAMS cyber-physical test bed is capable of simulating various sizes of power systems and creating datasets without altering the hardware configuration. A WAMS architecture is presented to demonstrate the integration of various components. Also, a wide variety of cyber-physical scenarios, dataset development process, selected results, specific and general test bed applications are presented.

2.2 Motivation

Power system blackouts are a result of sequences of events due to cascading failure [20]. From the past studies, it is known that a common initial cause of these large blackouts is a component failure which creates a chain reaction that leads to cascading failure. One of the prime reasons system operators were not able to take preventive and corrective control actions was due to lack of sufficient real time power system state information [20]. The initiating factors of such component failures can be natural causes such as power system faults, weather related events, seismic events or due to human error, uncoordinated maintenance, and cyber-attacks [21]. The evolution of GPS enabled phasor measurement units (PMU) which are an essential component of wide area measurement systems (WAMS) improves the real time information systems and provides a paradigm shift in the area of power system monitoring, control and protection. PMUs with incorporated protective relaying functionalities provide unprecedented advantage in wide area visibility, monitoring, control and protection of the bulk power system; thus improves situational awareness and better control. Though, these modern technologies

provide many advantages, the communication infrastructure and protocols used in monitoring power system states introduce many cyber-security issues.

Cyber security issues in industrial control systems have long been discussed. Recent cyber-attacks on various industrial processes have provided some insight to the potential impact of an attack against critical infrastructures. The Aurora attack on a generator demonstrated that vulnerabilities in protection schemes can be exploited to cause serious damage to power system components [22] [23] [7]. Liu et al. [24] presented random false data injection attack and targeted false data injection attack. Bobba et al. [25] proposed a method to detect false data injection attack described by [24] by protecting key measurements and H matrix. Similarly, modeling and countermeasure of false data injection attack is presented in [9] [10]. A different kind of attack called switching attack is presented in [26] [27] [8]. A variable switching theory is used to create coordinated control switching attack where an attacker takes advantage of corrupted communication channel and control signal of associated switch. Wang et al. [11] presented a survey on cyber security in smart grid. The paper presents several aspects of cyber-attack against smart grid such as attack denial of service (DoS) attack that can happen to different communication layers. DoS attack can be performed on physical layer, MAC layer, Transport layer, network layer and application layers. Some of the attacks are jamming in substations, ARP spoofing, buffer flooding and traffic flooding. The aim of the attacker may be violating any one of the three security objectives: Confidentiality, Integrity and Availability.

Various entities such as national labs, universities, research centers and utilities are focusing research on cyber security issues related to power grid vulnerabilities and

attacks. Multiple test beds and tools have been developed to study vulnerabilities, existing threats and impacts on system. The National SCADA Test Bed at Idaho National Laboratory is used to discover and address vulnerabilities and threats that exist in energy delivery systems [28]. Sandia National Laboratory has developed the virtual control system environment (VCSE) to study cyber threats on control-system dependent infrastructures [29]. Hahn et al. have developed a cyber-physical security test bed used to model isolated and coordinated attacks and to study the cyber-physical impacts using system's voltage and angle stability [30]. The virtual power system test bed and inter-test bed integration is used to evaluate the security performance of SCADA protocols and equipment [31]. The critical utility infrastructural resilience (CRUTIAL) test bed was developed to evaluate malicious threats on the grid control scenarios [32]. Finally, the SCADAsim test bed was developed to facilitate a simulation environment to test the security solutions and attacks on real devices and applications [33]. Most existing test beds focus on SCADA security and none of the existing test beds were developed to be used for research on Wide Area Measurement Systems (WAMS) security. Also, existing test beds do not cover a wide variety of cyber-power scenarios. There is a lack of a comprehensive cyber-physical test bed which provides a common platform to study various power system and cyber system interactions especially focusing on the emerging synchrophasor based WAMS. One of the contributions of the research work is development of WAMS cyber-physical test bed that include all essential components of a WAMS architecture and provides a platform to study cyber security issues on WAMS.

WAMS measurements are envisioned as very useful information to create various monitoring, control, and decision making tools for better situational awareness. Machine

learning algorithms and data mining techniques can replace traditional complex math based decision support systems which take longer time to provide results. The data mining algorithms can be used in developing events and intrusion detection systems (EIDS). Various event detection and intrusion detection systems are proposed in the literature especially focusing on using communication network related data. The use of synchrophasor data as sensor in EIDS to date has been minimal. Dahal et al. studied the possibilities of application of only synchrophasor data for power system event detection to aid better situational awareness [34]. Classification and regression trees (CART) data mining tool is used to characterize the signature of impending island formation in [35]. Similarly, decision trees (DT) based data mining techniques are used to study oscillatory and voltage stability events, and dynamic security assessment is performed based on the ensemble based DTs [36] [37]. All of these research work focused on power system events only. Pan et al. used a data mining technique on heterogeneous datasets to create common paths which are used as rules in intrusion detection system (IDS) [38] for power system.

These machine learning and data mining algorithms require a large amount of data to train and test algorithms. Robust event and intrusion detection will help mitigate potential cascading failures and cyber-attacks against power system infrastructure and maintain service availability, data confidentiality and integrity. The EIDS should be able to distinguish between the normal contingencies and control actions, and cyber-physical attacks against cyber-power critical components. However, authors in [39] point out there is lack of appropriated datasets for data mining researches. There are only handful of publicly available datasets and these datasets are relatively small in size. Power system

operation related datasets are not available. In addition, there is lack of data logs associated with a wide variety of events and hence, data related to these events are extremely difficult to obtain. Large blackouts, cascading failures, and cyber-attacks are very rare events and datasets related to such events almost impossible to obtain even from the utility. Also, datasets from utility are difficult to obtain due to propriety nature of the data and confidentiality issues, a non-disclosure agreement (NDA) is required in most cases. Since, these scenarios are impossible to implement in the real system, computer aided modeling and simulation is a better alternative to simulate and generate the datasets. Another contribution of the research work is development of big heterogeneous datasets with wide variety of cyber power scenarios to evaluate robustness of various data mining algorithms.

This chapter presents a cyber-physical test bed that integrates industry standard software, hardware and communication protocols; and which is designed to simulate wide variety of power system faults, normal power system contingences, control actions, and cyber-attacks against power systems. Also, this chapter presents a process to create heterogeneous dataset from various data sources including PMU, relay event logs, energy management system (EMS) logs, and network transaction logs. The remainder of this chapter is organized as follows. Section 2.3 presents the WAMS cyber-physical test bed and its components. Section 2.4 presents the implemented cyber-power scenarios. Section 2.5 presents the dataset development process, and section 2.6 presents test bed applications.

2.3 Development of WAMS cyber-physical test bed

This section presents the implemented WAMS cyber-physical test bed. The test bed architecture is shown in Figure 2.1. The test bed consists of physical systems, communication infrastructures, and control and monitoring functions. The hardware, software, and communication protocols used in the test bed are industry standard the hardware in the loop (HIL) and software in the loop (SIL) implementation of relays, PMUs, PDC, protocols, and software facilitates cyber-attacks and real world power system scenarios such as faults and contingencies. The implementation of WAMS facilitates *big heterogeneous dataset* creation. The WAMS cyber-physical test bed captures the essence of a wide area measurement systems (WAMS) and is small enough to be comprehensible in every detail. The test bed and datasets exhibit features of a real power system, yet the system fits into resources available in the lab in terms of hardware and software limitations. Each component is briefly presented here.

2.3.1 Physical systems

The physical power system is simulated using a real time digital simulator (RTDS). The RTDS is able to emulate electrical machines, controllers, transmission system components, and system load accurately and also provides a hardware in the loop (HIL) simulation environment. The integration of virtual, simulated, and actual hardware components in HIL in the test bed captures the essence of the entire power system operation. The size of the system is limited by the RTDS hardware, however, the modeled systems closely mimic real power system behaviors.

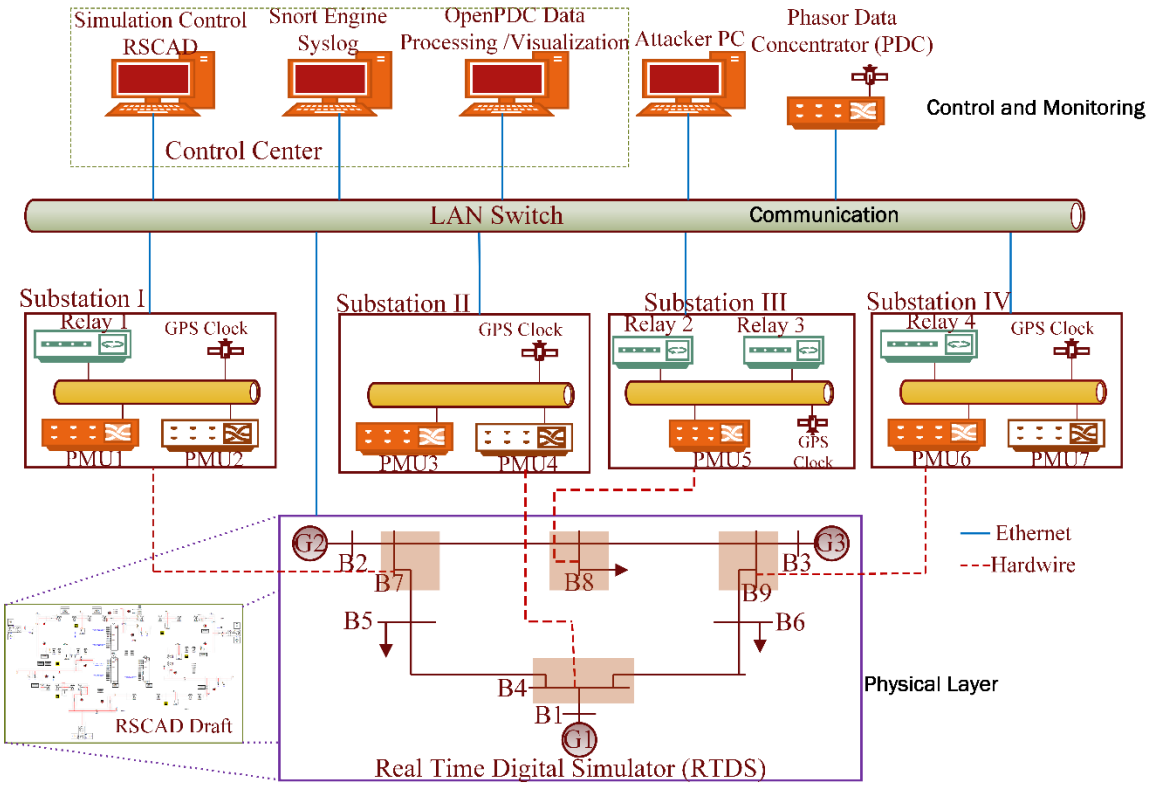


Figure 2.1 WAMS architecture

As an example, the WAMS architecture that implements the WECC nine bus system is shown in Figure 2.1. Each modeled substation is equipped with either hardware relays or software relays or a manual breaker control mechanism for simulating contingencies and attacks. The location of hardware relays was chosen strategically to enable simulation of important cyber-attacks, control actions, and contingency scenarios. Also, each substation is equipped with PMU(s).

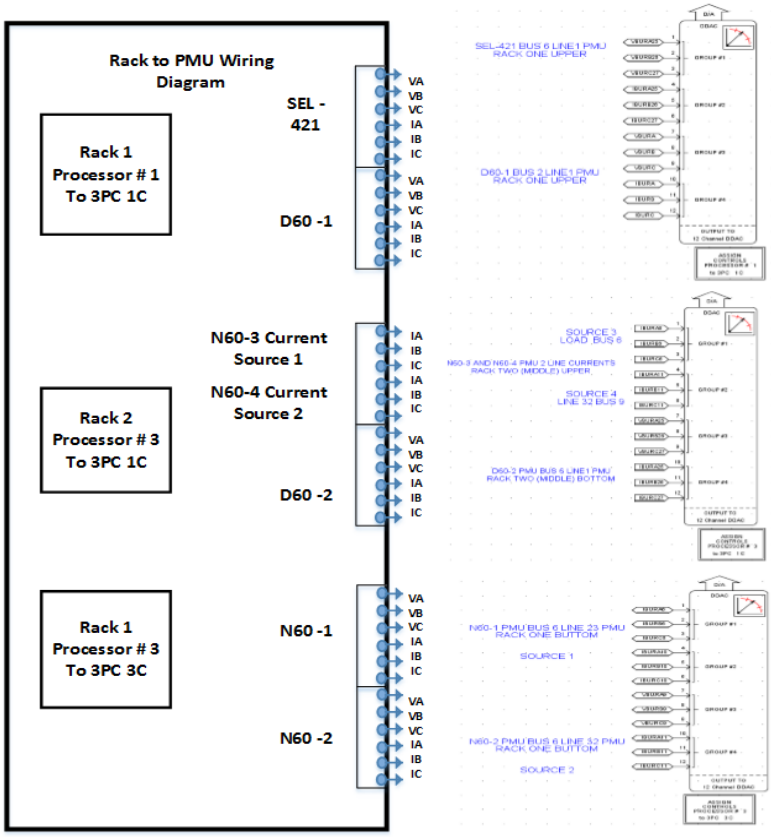


Figure 2.2 PMU assignment on the RTDS back plane on the left and RSCAD interface on the right

One of the most important physical components of the WAMS test bed is PMUs that create an effective WAMS. The test bed consists of seven hardware PMUs from different vendors. The configuration of PMU and their placement can be changed within RSCAD modeling. Hence, the test bed provides moderate scalability and flexibility for PMU placement in the system. The test bed also consists of hardware relays. These PMU and relays are hardwired from RTDS back plane. The actual physical assignment of these seven PMUs on RTDS backplane is shown in Figure 2.2. The RTDS consists of two racks. Rack one incorporates four PMUs (SEL-421, GE D60-1, GE N60-1, and GE N60-

2) and rack two incorporates three PMUs (GE D60-2, GE N60-3, and GE N60-4). Also, three physical over current and distance protection relays are incorporated in the system. The remaining required relays are modeled as software relays. In addition, the test bed consists of a hardware Phasor data concentrator (PDC) and all PMUs are configured to stream data to the PDC.

Currently, the test bed can simulate 5 different power system models; a three generator four bus system [40], a modified two generator three bus system, a WECC nine bus system, a two area power system [41], and the IEEE fourteen bus system. These power system models can be used for various applications discussed in test bed applications sections.

The accuracy of simulation depends upon accurately modeling of a system. To ensure model accuracy, three validation steps were performed for each model. First, PowerWorld© and RSCAD solution were compared. Second, the output of the developed system was compared with the output presented in the literature whenever possible [40]. Finally, the values obtained during the simulation were compared with the PMU data. Simulated power system models were found to be accurate.

Significant challenges to identify proper I/O interface were overcome and proper scaling of the PMU inputs are calculated so that the RTDS I/O output signal level is not over saturated. The scaling is calculated following guidelines provided from RTDS [42] and fine-tuned manually. Validation of Phasor quantities during steady state and dynamic condition was achieved by comparing signals from RTDS runtime windows and PMU measurements. The waveform shown in Figure 2.3 is a phase A bus voltage measured by PMU (blue line) and RTDS (red line) during the single line (phase A) to ground fault on

a transmission line. The waveforms are found to be close to identical as shown in Figure 2.3.

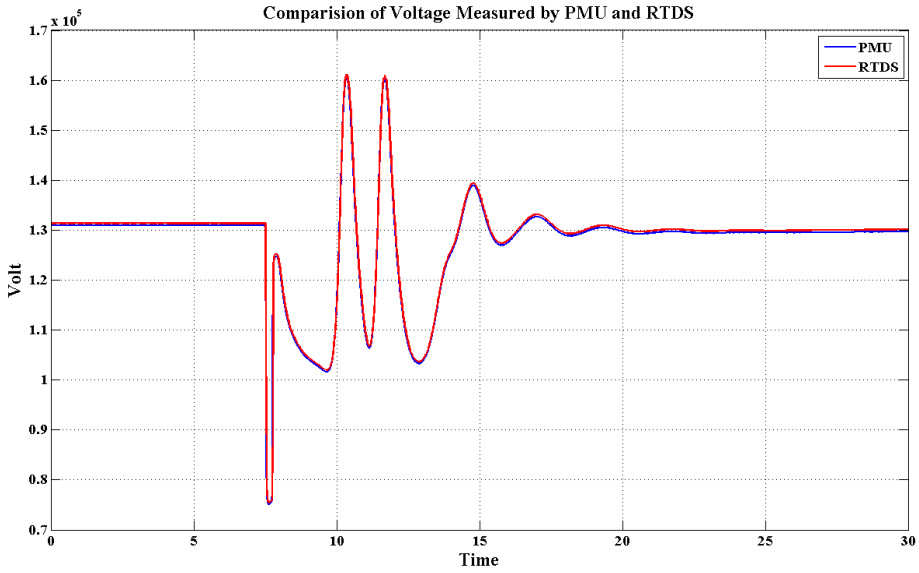


Figure 2.3 Comparison of voltage measured by RTDS and a PMU

2.3.2 Communication infrastructure

The communication infrastructure in the test bed includes a physical network, communication protocols used for transporting measurements, and control signals from device to device and between control centers and substations. The RTDS, PMUs, PDC, relays, Snort engine, OpenPDC, attacker PC, and historian are connected via a network switch which supports copper and fiber optic connections. RTDS and other substation devices such as relays and PMU communicate using various network protocols including MODBUS, Telnet, TFTP, DNP3, IEC 61850, and IEEE C37.118. The main communication protocol used for wide area based monitoring system is IEEE C37.118. MODBUS and Telnet are used to adjust device configuration and settings [43].

2.3.3 Monitoring and control applications

The test bed monitoring and control components include hardware PMUs, PDC, and relays, a data processing engine, and industry standard software. The relays, PMUs, and PDC setting are configured and system status is monitored using software packages from General Electric (GE) and Schweitzer Engineering Laboratories (SEL). Wireshark and Snort are used as network monitoring and analysis tools in the test bed. The PMUs are configured to stream synchrophasor data to a GE PDC with data rates up to 120 samples per second. The test bed includes both a hardware and software PDC. A GE hardware PDC congregates measurements from each PMU according to time stamps, extrapolates for missing and corrupted values, and forwards concatenated measurements to the historian. Open source software PDC called OpenPDC collects synchrophasor data from hardware PDC. The dataset development process is presented in section 2.5 in detail.

At the substation level, local control is employed using a hardware-in-the-loop (HIL) configuration using relays. Over current and distance protection relays are implemented to control the breakers for faults and other disturbances in the system. Hence, the test bed incorporates centralized and local controls with industry standard software and hardware to simulate the system, collect measurements, collect device status from field devices, forward operator commands to field devices, and manage historic data.

2.4 Test bed scenarios

2.4.1 Power system faults, contingencies, and control actions

Symmetric and unsymmetrical faults in a power system are considered as the examples of disturbances. A power system fault is a condition where the system voltage, current and frequency are abnormal. Typically, single line to ground (1LG) faults (70%), double line to ground (2LG) faults (10%), three lines to ground (3LG) faults (5%), and line to line (LL) faults (15%) represent greater than 95% of faults in a power system [44]. In this work, phase-a-to-ground fault for 1LG faults, phase-*a*-*b*-to-ground faults for 2LG faults, phase *a*-*b*-*c*-to-ground fault for (3LG) faults, and phase-*a*-to-*b* line to line fault for LL faults are simulated. Coordinated distance protection schemes is implemented using hardware relays in HIL environment. Each relay provides primary protection up to 80% of the line (Zone 1 protection) and backup protection (Zone 2 protection) up to 150% of the line. The trip time for Zone 1 protection is set to instantaneous while the trip time for the Zone 2 protection is set to 20 cycles. The details of the protection scheme implementation can be found in [45]

The dynamic contingency analysis re-defines the traditional contingency analysis techniques and takes into account of the protection equipment operation in real time. The dynamic contingency analysis is simulated by opening the breakers in the system and the impact of these operations on the system will be evaluated for security analysis [46]. These breaker operations may be simulated due to protection device actions, manual operations, and cyber-attacks. Since, the developed test bed is equipped with relays in HIL environment, realistic relay operation and breaking operation during faults and other abnormal operating condition is possible. Similarly, the power system models are

equipped with manual switches and attack scripts, manual breaker operation and cyber-attacks initiated breaker operation is achieved.

Currently the test bed is capable of simulating generator loss, change of generator output, transmission line in and out of service, and load change or loss. The aforementioned contingencies can be simulated singularly to create N-1 scenarios and combinations of the contingencies can be simulated to create N-K scenarios in real time. Table 2.1 summarizes the scenarios simulated in the test bed.

Table 2.1 Power system contingencies and control actions

Scenarios	Sub-categories
Shunt faults	Single line to ground faults Line to line faults Line to line to ground faults Three phase faults
Load variation	Load can be changed dynamically
Load loss and recovery	Loads can be switched on and off
Generator loss and recovery	Circuit breaker can be switched on and off as schedule outage or attacks
Transmission line loss or recovery	CBs can be opened and closed as maintenance and attacks

2.4.2 Cyber-power system attacks

Power system attacks may originate from insiders, amateur hackers, political activists, criminal organizations, governments, and terrorists. Cyber-attacks may appear as a nuisance or may bring the system to collapse [47]. Attacks could be carried out by physically harming the system components, by exploiting weak security policies of premises such as substations, control centers, and transmission and distribution

infrastructures. Similarly, skilled attackers may take advantage of security flaws and vulnerabilities in software, devices, communication infrastructures, and protocols.

Within the substation level there are several points where an attacker can craft attacks on data integrity and availability. The cyber-attacks may involve control command injection, response injection, and denial of service (DoS) attacks. The control command injection attack can be used to control the devices and change the configuration. The response injection attack consists of sensor data fabrication and data alteration. These types of attacks may cause false breaker operation, EMS application failure, system outage, false alarms, and cause system limit violations. In WAMS architectures, substation relays are vulnerable to command injection attacks and physical attacks. Also, PMUs in substations are vulnerable to network attacks. An attacker may craft attacks such as false response injection and denial of service (DoS). The attacker can target an individual PMU or relay. However, an intelligent attacker can create coordinated attacks on many relays and PMU simultaneously.

Since, these intelligent electronic devices (IED) are connected to the control center or a higher level aggregator using high speed communication network, it is possible to create attacks on data integrity and availability. An attacker can inject commands which mimics the command from control center. Also, various response injection attacks are possible between phasor data concentrator (PDC) and control center. These types of attacks are even more dangerous as they affect large number of PMU streams. The impacts of such attacks are loss of services, cascading failures, complete or partial loss of visibility, and limited or skewed situational awareness. All the data integrity attacks affect various EMS applications such as state estimation and

contingency analysis which ultimately causes incorrect control actions. Figure 2.4 shows different possible attack points in WAMS. The attacks can be on physical system, between the sensor measurements, and applications.

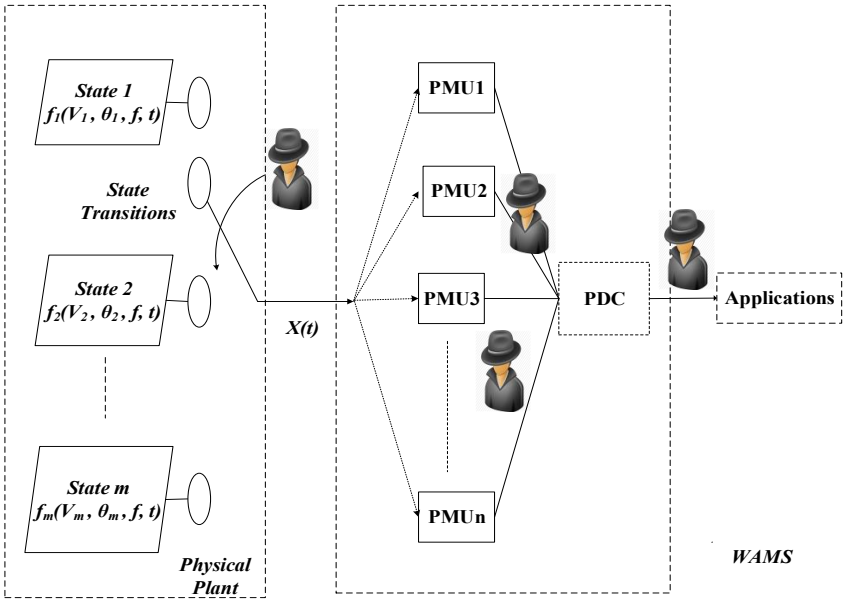


Figure 2.4 WAMS attack points

The hardware in the loop (HIL) and software in the loop (SIL) setup in test bed is key to create command injection and man in the middle attacks. HIL and SIL provides key attack points and tools to create more realistic attacks. In this study, it is assumed that an attacker has penetrated into the substation. Hence, substation targeted attacks are considered. The test bed can simulate attacks from each of the aforementioned categories listed in Table 2.2.

Table 2.2 Cyber-physical attack scenarios

Types of attacks	Sub-categories
Command injection attacks	Command injection to relay Aurora attack
HMI/UI attacks	Relay setting changes Disable relay Remote trip and reclose
Man in the middle attacks	Data corruption False data injection Replay attack
Physical attacks	Relay shutdown Connection changes UTC time vandalism
Denial of service	Data flooding MODBUS and IEEE C37.118 Protocol Mutation

Command injection attacks are available to create contingencies. Relays can be tripped by remote command injection attack. Relays from two vendors are available in the test bed. Attacks are available to remotely trip both types of relays. In both cases a network packet capture tool was used to capture a command which is used to remotely trip the relay. In the attack scenario these commands are replayed on the network from an attacker PC connected to the network switch. Aurora attack is repeated command injection attack on relays to open critical breakers.

Man-in-the middle (MITM) attacks can be used to emulate faults and contingencies. The MITM attacks alter power system measurements transmitted from field devices to control room systems. Implemented MITM attacks include a false data injection attack which alters current and voltage Phasor and replay attacks which resend captured PMU frames from a previous period. Both of these attacks can be used to confuse an operator or automate algorithm monitoring the systems. Faults, generator loss,

load changes, and transmission line loss can be replayed. The SLG fault replay attack attempts to emulate a valid fault by altering system measurements to mimic a SLG fault followed by sending an illicit trip command from a compromised computer to relays at the ends of the transmission line

Physical attacks may consist of relay shutdown, connection changes, UTC time vandalism, Insiders may also physically trip a relay from the face plate and change settings.

HMI and UI attacks are provided to simulate invalid changes to relay settings. These relay settings changes include change setting parameter threshold and relay operating time values as well as disabling the relay completely. HMI and UI manipulation attacks are automated by an AutoIT script. Such attacks mimic effects of insiders taking illicit control actions and malware taking control of software systems to manipulate control devices.

Finally, two varieties of DOS attacks are available. First, scripts are available to send high volumes of network traffic (floods) to a network target in attempt to overwhelm network processors and memory. Second, two Python based protocol mutation engines are available to send mutated packets. The first protocol mutation engine randomly flips bits in network packets. The second protocol mutation engine sends intelligently manipulated packets.

Results from three cyber-attacks are described below as example demonstrations of test bed capabilities. Figure 2.5 shows the result of MITM attack in which an attacker randomly alters current Phasor in a PMU stream. The range of current for the normal operation in this case is between 200 and 550 Amps. The graph shows current values for

different load scenarios. From the time 21:12.6 to 21:30.1, the attacker is able to inject random current values. This attack is carried out between a PMU and PDC. The attack script is able to inject any random data or coordinated false data into the system. Any number of PMUs can be attacked in these scenarios.

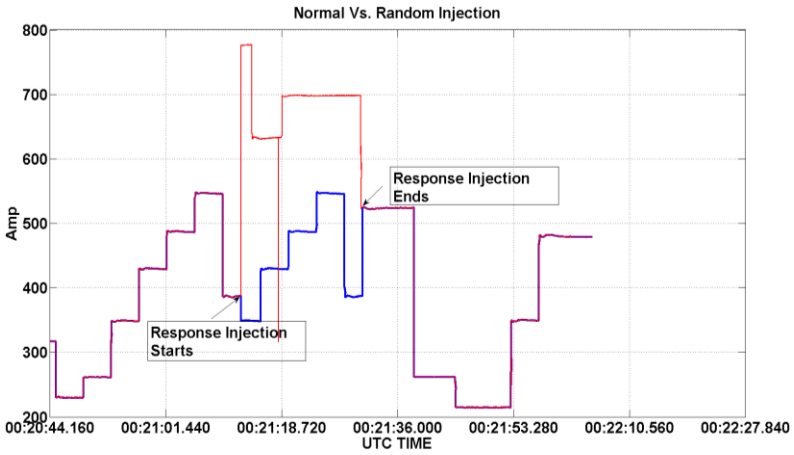


Figure 2.5 Man in the middle attack against PMU 4

Figure 2.6 shows a PDC's query response time while the device is subjected to a DOS attack with an increasing flood of network packets. The brown triangle shows the rate of transmitted packets, blue lines shows device response times, and red dots show response timeouts. The flood causes a loss of communication which in turn leads to loss of system monitoring capability.

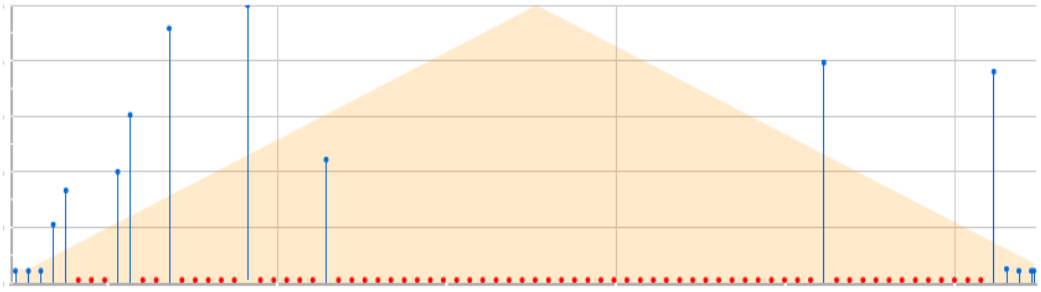


Figure 2.6 Denial of service response

Figure 2.7 shows the result of an attack against the coordinated distance protection scheme in which an attacker takes control the relay's control room client or HMI and changes a setting to disable the relay. Due to the setting change the relay does not operate for a severe fault. This type of attack can have significant impact on system protection if the fault duration in the system is longer than that shown in the figure. Some faults must be cleared within a pre-specified time to maintain generator synchronism and to avoid damage to system components such as transformers.

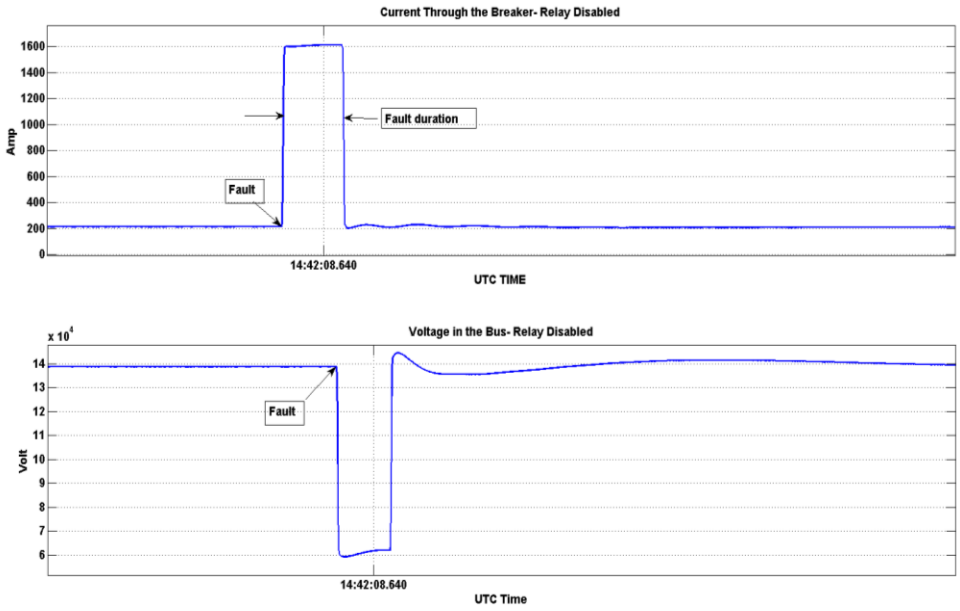


Figure 2.7 Relay operation failed during fault due to relay setting change

2.5 Dataset development

Especially, the data mining research community is facing challenges to obtained appropriate datasets for evaluating algorithms [19]. There are few publicly available repository sites where researchers can obtain datasets. However, power system related data are not available in such repositories [48] [5]. Also datasets related to scenarios such as cascading failure, large blackouts, and cyber-attacks are very rare and obtaining data related to such events is extremely difficult.

Datasets should include contingencies, variety of faults, control actions, and cyber-attacks in a random order. Also, it should include random variation of load and location of the events. Data plays an important role to develop an effective EIDS that can be used to classify cyber-power events. Power system operation is very dynamic where scenarios are constantly evolving. The load variation, occurrence of disturbance and its

location, contingencies, control actions, and possible cyber-attacks are very random in real power system operation. EIDS must be robust to be able to distinguish wide variety of events. In order to ensure the robustness of the data mining methods, the algorithms should be evaluated with the datasets that includes random events which closely mimic real power system operations.

The second requirement on datasets is that the test bed should be able to provide robust heterogeneous datasets that include synchrophasor measurements of physical system states, monitoring, control and protection devices logs, Control panel logs, and network transaction for various applications. The need of heterogeneous datasets in the context of development of EIDS is critical. Usually power system researchers do not require other than PMU measurements for event detection methodology development. For example, Dahal et al. evaluated various data mining algorithm using synchrophasor measurements only [34]. However, in EIDS other information are very important to distinguish whether particular event is natural power system event or the cyber induced incident. For example, if only synchrophasor measurements are considered to develop EIDS, it may not identify the difference between the real SLG fault and SLG fault reply attack because a PMU provides identical system state signature for both events as shown in Figure 2.8. But if other information are incorporated in the datasets, this will provide additional fidelity to the detection system. A simulation control and data integration engine is developed to achieve the automated simulation control and create heterogeneous datasets with random scenarios which is presented in the next section.

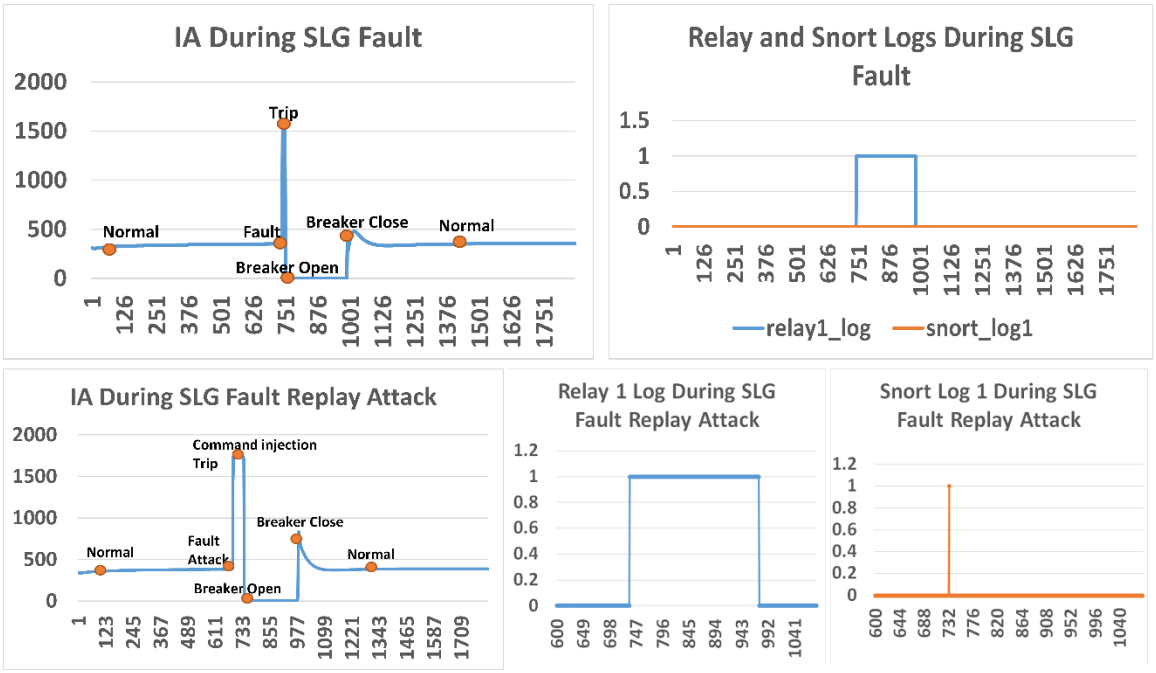


Figure 2.8 Sequence of cyber-power events

2.5.1 Simulation control and data integration engine

Figure 2.9 shows the interaction between various elements in the simulation control and data integration engine. The AutoIT script is a master control which governs three sets of subtask scripts: attack scripts, MATLAB scripts, and control panel scripts. AutoIT master control schedules the random scenarios from these three categories. The attack scripts simulate the cyber-attacks. The MATLAB script simulates power system faults with variation in types of fault, fault location, fault duration, and fault resistance. The control panel scripts simulate contingencies such as transmission line loss (recovery), generator loss (recovery), and scheduled maintenance by opening and closing the circuit breakers.

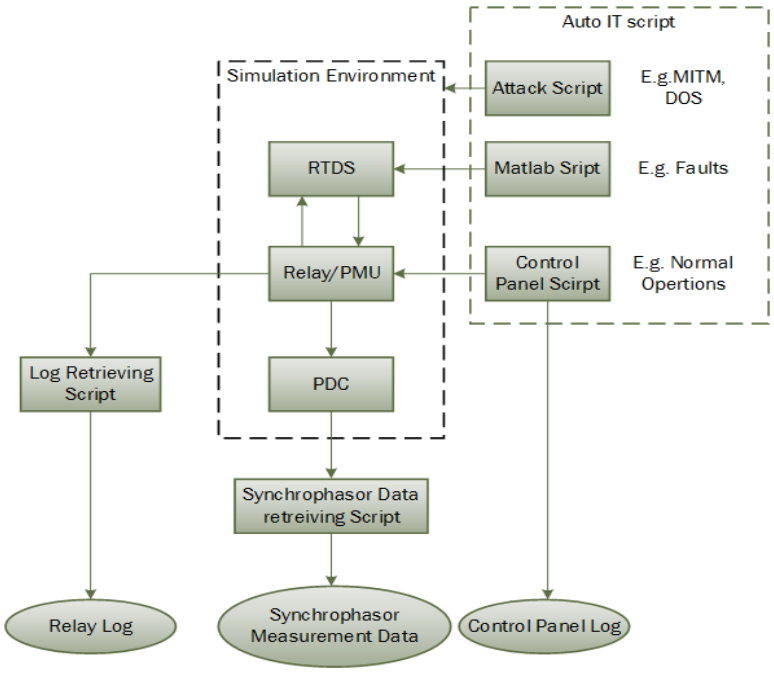


Figure 2.9 Simulation control and data integration engine

A second set of scripts collect data from OpenPDC, relay logs, Snort, and control panel. These scripts are used to create heterogeneous datasets. Synchrophasor data retrieving script translates synchrophasor data to Comma Separated Value (CSV) format. The EMS and control panel logs retrieving script, relay logs retrieval script, and snort retrieving script up samples the discrete event logs and aligns the data with corresponding timestamps. A master script merges all the datasets into one CSV file. Summary of dataset integration and development is shown in Figure 2.10. The datasets are defined as "*heterogeneous datasets*" because the source, format of the data, and rate of data stream are different. For example, a PMU and custom calculation engine provide continuous electrical measurement data at the rate of 120 samples per second. But, the control center, relays, snort engine provide event driven discrete data with variable rates.

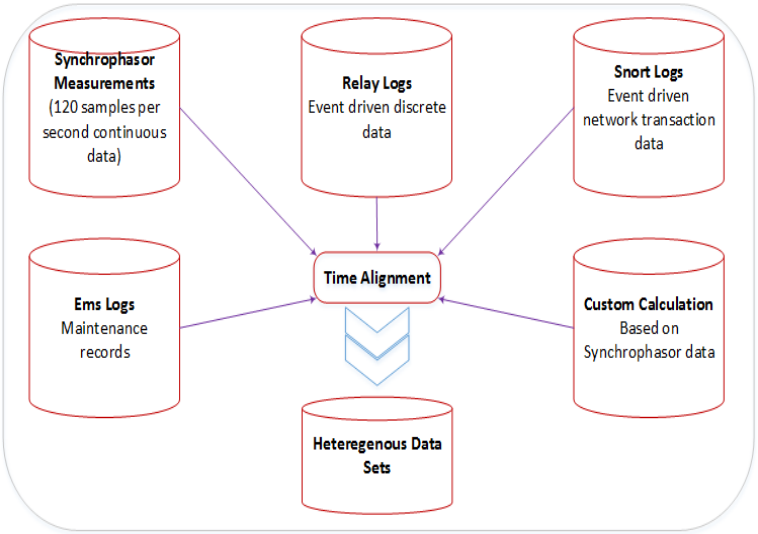


Figure 2.10 Dataset integration and development

2.5.2 Dataset examples

A two generator, three bus system with two transmission lines with a variable load system was created by modifying a three generator four bus system [40]. This system was modified to meet the requirements of the proposed task that simulates a coordinated multi zone coordinated distance protection scheme. Figure 2.11 shows single line diagram (SLD) of the modeled system implemented on a real time digital simulator (RTDS) [42].

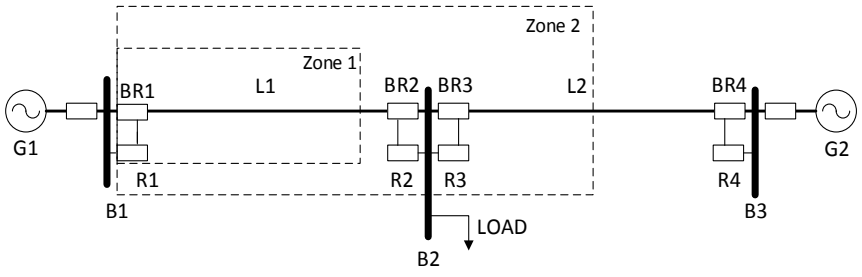


Figure 2.11 Single line diagram of the power system

G1 and G2 provide the necessary power to balance load at bus B2. PMU 1-4 are embedded in relays R1-4 respectively and provide bus voltage and line current phasor. PMU 5 is placed at bus B2 and measures load current phasor. Relays R1 and R2 protect line L1 by opening breaker BR1 and BR2, and R3 and R4 protect line L2 by opening breakers BR3 and BR4.

The primary dataset developed in the lab consists of 10,237 instances of scenarios randomly simulated among 41 cyber-power scenarios and defined as *'dataset 1'*. The size of the heterogeneous dataset is approximately 34.7 GB. These datasets have used in various research studies [49] [38]. These scenarios consist of single line to ground SLG fault at variable locations in 1% increment from 10% to 90% on transmission line L1 and L2 (Q1-Q6), SLG fault replay attack on line L1 and L2 (Q7-Q12), line L1 and L2 maintenance (Q13-Q14) that mimics the scenario when an operator remotely trips relays to open breaker at both ends of transmission lines, command injection against single relay (Q15-Q18), command injection against two relays (Q19-Q20), primary protection single relay disabled attacks with SLG fault (Q21-Q30), single relay disabled attacks and line maintenance (Q31-Q34), two relay disabled attacks and fault (Q35-Q38), two relay disabled and line maintenance (Q39-Q40), and finally normal power system operation (Q41). The load is changed randomly from 200-400 MW.

The relay command injection attack was used to create contingencies by sending trip commands to relays to open breakers at the end of transmission lines L1 and L2. The attack originates from a remote computer with a spoofed IP address. Only the SNORT network monitor detects the trip commands associated with this attack. Since the attacks originate from another computer, there will be no control panel logs as with a legitimate

line maintenance scenario. This attack mimics a legitimate line maintenance scenario. Versions of this attack targeted individual and pairs of relays.

The single line to ground (SLG) fault replay attack is a combination of a man in the middle (MITM) attack and a command injection attack. For the SLG fault replay attack, the attacker emulates a valid fault by altering PMU measurements followed by an unauthorized trip command injection sent to relays to open breakers at the end of lines L1 and L2. The measurement alteration is done between the PDC and historian computer using a python script and Ettercap. SLG fault replay attacks were performed at random locations on line L1 and L2.

The disabled relay attack simulates the conditions in which settings of control devices are changed without authorization. The setting can be changed by insiders or malware taking control of software systems. A MODBUS/TCP command sent from an attacker's computer modifies the relay settings to disable relays and prevent relays from operating during fault conditions and line maintenance. Individual and pairs of relays were disabled.

Each scenario starts from a normal operation state, then the event occurs, and finally the system returns to normal operation. The scenarios are labeled with 'Q' followed by a number and list of the scenarios is presented in the appendix A.

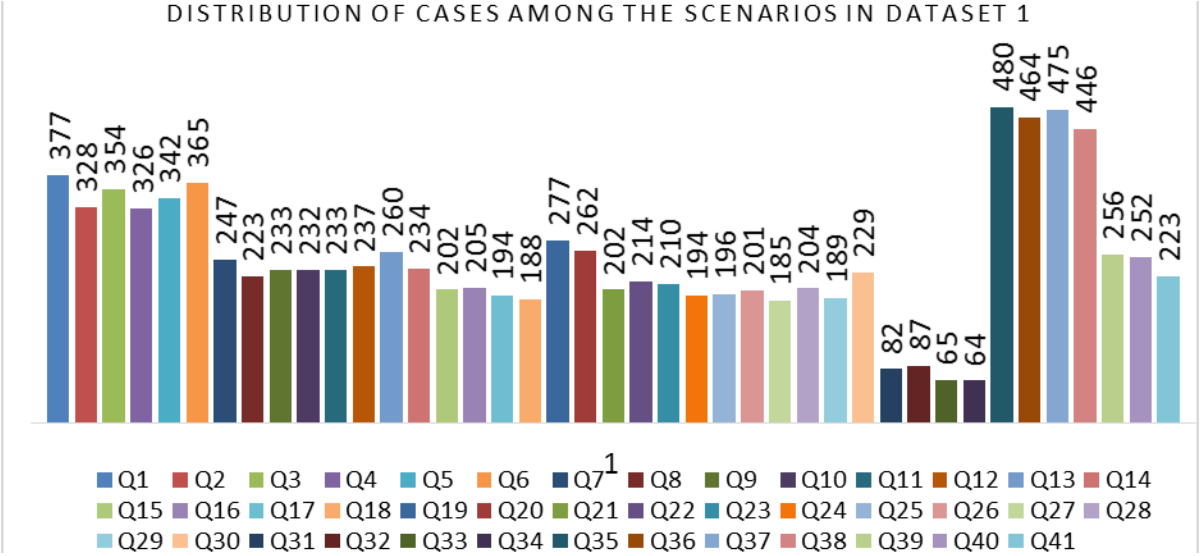


Figure 2.12 Distribution of cases among the scenarios for dataset 1

The distribution of the 10,237 instances is shown in Figure 2.12. Each bar represents the total number of cases in one scenario.

Another dataset of size 38.3 GB was also created by adding additional scenarios and defined as *'dataset 2'*. The added scenarios include double line LL fault on line L1 and L2 (Q102), double line to ground 2LG fault on line L1 and L2 (Q108), three phase to ground 3LG fault (Q114), and repeated command injection attack called 'Aurora attack' to relay R1 (Q119). Each fault was simulated at a random location in 1% increment from 10 to 90% on transmission lines L1 and L2. The total number of scenarios in this dataset is 45. Each bar represents the number of cases in each scenario as shown in Figure 2.13. The total cases in this dataset is 11,715.

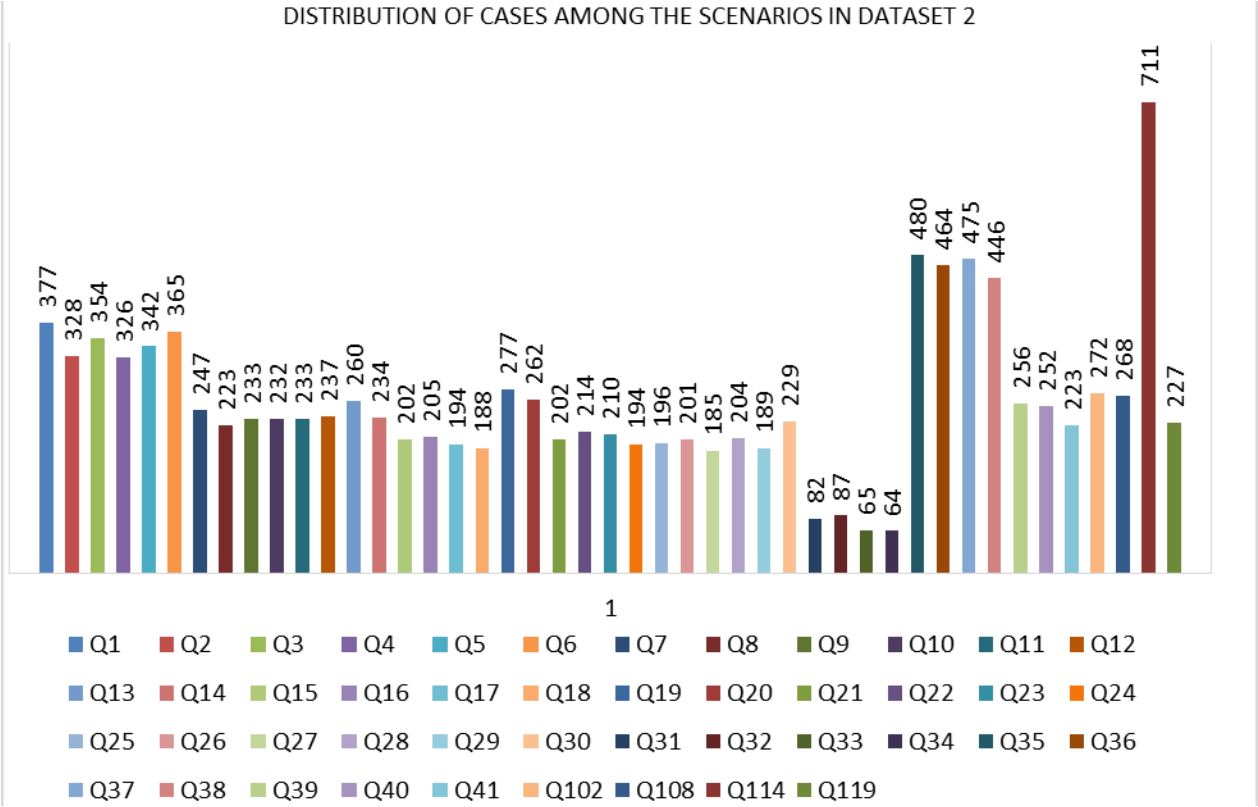


Figure 2.13 Distribution of cases among the scenarios for dataset 2

2.6 Test bed applications

The test bed has been used to create datasets for a large number of research projects. These datasets have been used by researchers at Mississippi State University, Oak Ridge National Laboratory, and University of West Virginia. These use cases are described below.

2.6.1 Evaluation of data processing method and development of event and intrusion detection systems (EIDS)

The dataset described in section 2.5.3 was used to develop a data size reduction technique which is presented in Chapter 3 and is called the STEM algorithm. The STEM algorithm reduces the size of large heterogeneous power system data significantly while

maintaining key patterns in the data. Two datasets of size 34.7 GB and 38.3 were created with 41 and 45 cyber-power scenarios.

Similarly, these datasets were used to evaluate classification accuracy of an EIDS built with the NNGE data mining algorithm. The NNGE based EIDS is presented in Chapter 4 in detail.

Additionally, these datasets were used to evaluate an online EIDS which is based on Hoeffding Adaptive Trees (HAT). The details of the online EIDS is presented in Chapter 5.

2.6.2 Synchrophasor data dimension reduction techniques

The test bed was used to generate the datasets required to evaluate the dimensionality reduction of synchrophasor data using principle component analysis (PCA) [50]. A three bus four generator power system [51] based on [40] was used to create datasets which included 18 measurements from two PMUs.

2.6.3 Data stream mining

Researchers in [34] evaluated the performance of Hoeffding tree based data stream mining techniques for static and evolving data streams. The test bed was used to create synchrophasor datasets with various power system events to simulate concept drift in power systems [51].

2.6.4 Machine learning for power system disturbance and cyber-attack discrimination

In [49], researchers explored the viability of traditional machine learning methods to classify power system disturbances and cyber-attacks. The test bed was used to create

datasets for algorithm evaluation. The datasets for this work included data from heterogeneous sources such as PMU measurements, apparent impedance seen by relays, Snort logs, relay logs, and Control panel logs.

2.6.5 Dimension reduction using mutual information optimization

Researchers in [34] presented a method to select the features of synchrophasor measurement based on mutual information. The test bed was used to create synchrophasor datasets to validate the developed method [51].

2.6.6 Common path mining for faults and cyber events in power system

A data mining algorithm to mine common paths for fault and cyber events detection in power system was evaluated in [38]. The modified two generator three bus system test bed was used to simulate short circuit faults and command injection attacks which remotely trip relays.

2.6.7 Hybrid intrusion detection systems using data mining technique

A hybrid intrusion detection system for power system was evaluated using the datasets. In this study SLG faults, line maintenance, relay trip command injection attack, relay disable attack, SLG fault replay, and variants of all scenarios were simulated. In both cases, heterogeneous datasets were created from different sources such as PMU measurements, relay logs, snort logs, Control panel logs, and apparent impedance are used [38].

2.6.8 Vulnerabilities assessment and impact study

2.6.8.1 Vulnerability assessment

The test bed was used to test WAMS devices for cybersecurity requirements conformance and test for vulnerabilities. The test bed was used to perform network congestion testing, denial of service testing, and protocol mutation testing [43]. The results of the tests were provided to the device vendor to allow them to create corrective actions [52] [53].

2.6.8.2 Impact study

Also, the test bed was used to study the impacts of cyber-attacks against a power system. A continuous command injection attack known as the 'Aurora attack' was simulated using IEEE fourteen bus system. The impact of cyber-attack was evaluated based on the variation of torque produced by the generator and power swing during the attack [54].

Cascading failures usually consist of voltage collapse phenomena in which a sequence of events lead to an unacceptable voltage profile to a significant portion of the power system. Usually, voltage collapse occurs when there is deficiency of reactive power support and reactive power demand is not met [41].

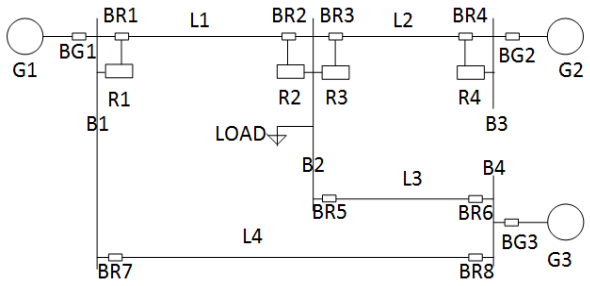


Figure 2.14 Three generator four bus system

A voltage collapse scenario induced by a cyber-attack was demonstrated using the three generator four bus system shown in Figure 2.14. Initially, the system is stressed and is operating at maximum load condition at P= 400 MW and Q= 60 MVAr and all transmission lines except line L4 are operating at nearly 80 % of the capacity. All lines are identical and their capacity is assumed to be 175 MW. The voltage at load bus B2 was monitored using a PMU. Before the attack, the bus voltage was 0.962 PU which is within acceptable range. The common acceptable voltage range is 0.95-1.05 PU. Other monitored parameters are shown in the Table 2.3.

Table 2.3 Active and reactive power generation and flow (in MW and MVAR)

Scenario	G1 [P, Q]	G2 [P, Q]	G3 [P, Q]	L1 [P, Q],	L2 [P, Q],	L3 [P, Q]	L4 [P, Q]
Normal	137.7, 12.11	134.3, 19.96	134.4, 11.97	136.4, 16.51	134.2, 12.95	133.5, 16.49	1.14, 11.43
After an attack	205.9, 35.2	202.4, 40.28	0, 0	136.5, 22.76	202.3, 23.51	68.50, 12.42	68.99, 12.41
After line loss	397.7, 237.6	0, 0	0, 0	263.8, 110.6	0, 0	130.6, 36.66	130.7, 36.68

A command injection attack was executed to open the generator breaker GB3. As the breaker opened, there was a brief voltage dip at the load bus as shown in the Figure 2.15. Within a short period of time, the voltage recovered to an acceptable value. The load was picked up by generator G1 and G2. However, transmission line L2 was overloaded due to the redistribution of power after the loss of generator G3. BR3 and BR4 open due to the overloading after a short period of time. The loss of the heavily loaded long line (L2) causes additional loading on the remaining lines L1 and L4. The loss of generator G2 and G3 forced the remaining generator G1 to supply the power demand. The reactive power demand is not met by a single generator, in an absence of control schemes and load shedding, the system suffered from a voltage collapse. The load bus voltage never recovered after the loss of line L2 as shown in Figure 2.15.

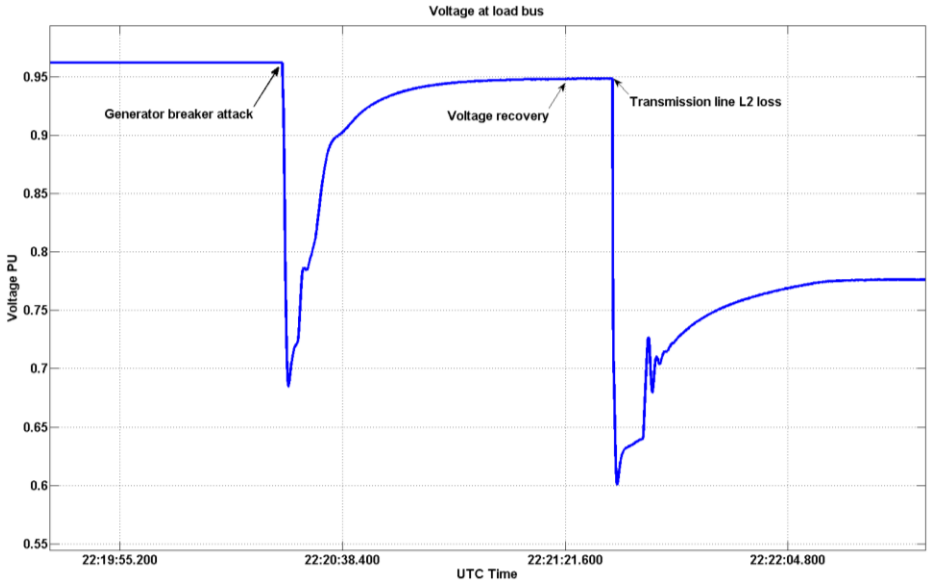


Figure 2.15 Cascading failure and voltage collapse due to a cyber-attack

2.7 Conclusion

Many contemporary research projects on power system event detection, data mining, data stream mining, cyber security, and vulnerability assessment in power systems are hampered by a lack of a suitable cyber-physical test bed and time synchronized heterogeneous datasets from WAMS. This WAMS cyber-physical test bed captures the essence of a wide area measurement system (WAMS) and is small enough to be comprehensible in every detail. The test bed and datasets exhibit features of a real power system, yet the system fits into resources available in the lab in terms of hardware and software limitations. The WAMS cyber-physical test bed developed by integrating industry standard components mimics a scaled version of WAMS. The test bed provides platforms to implement various cyber-power event scenarios and create heterogeneous datasets required to develop event and intrusion detection systems (EIDS) and other data mining algorithm evaluation. The implemented scenarios include natural power system events, control actions, and cyber-attacks. The data integration and simulation control engine automated the random event simulation and created big data for data mining. The WAMS test bed contributed in many research areas and became a significant component in a number of publications. The test bed has been used for impact studies in power systems due to cyber-attacks [54], vulnerability assessment of WAMS [43], data mining using Synchrophasor data [50] [34], machine learning methods in power systems [49], and intrusion detection in power systems [38]. This test bed was also used in this research to develop a data processing method to reduce large heterogeneous data, evaluate traditional batch processing data mining algorithms, and a data stream mining algorithm.

In future work, the test bed can be extended to study the different causes of cascading failures due to single or multiple element failures, power system cyber-attack scenarios and power system resiliency against cascading failures. The test bed has potential application in wide area protection system (WAPS) development and validation, digital forensics and cyber-security analysis, risk assessment, and attack modeling and defense. Although the RTDS based test bed has various advantages, scalability is difficult to achieve. A different approach of simulation of large system is necessary. Distributed simulation and Thevenin method are two potential approaches to deal with scaling issues.

CHAPTER III

DATA PROCESSING FOR EVENT AND INTRUSION DETECTION SYSTEMS (EIDS) IN POWER SYSTEM

3.1 Introduction

EIDS use synchrophasor data combined with data from other heterogeneous sensors to detect cyber-attacks and classify events. Synchrophasor streams are high velocity data streams. Training and classifying events using Synchrophasor data can require large amounts of memory. An example PMU which transmits 12 Phasor and 2 digital status words will create 96 bytes per sample period. At 120 samples per second a single PMU creates 11,520 bytes of data per second. Five hundred PMU spread across a system will create 19.3 gigabytes (GB) of data per hour and 463 GB in a day. Traditional batch processing data mining techniques are sensitive to memory and large data sizes [55]. As such, the volume of synchrophasor data fused with data from other sensors needed for an EIDS can easily exhaust a learner or classifier's available memory. Additionally, Phasor are real are or fixed point numbers which are treated as continuous by a learner and therefore lead to infinite state space. Hence, an effective data processing method is required to reduce the volume of data and limit the state space of during classifier training. This chapter presents a state tracking and extraction method (STEM) which uses sequential state tracking to reduce data volume and state space while maintaining key patterns needed for machine learning algorithms to classify events.

STEM allows the resolution of the data to be changed by changing the quantization interval.

EIDS make use of sensor data obtained from a variety of sensor devices in different data formats. The STEM algorithm consists of 5 steps. First, data is collected from the various sensors of interest to the EIDS. Second, sensor data from heterogeneous sensors is merged into a single file. Merging requires up-sampling of slower data streams to merge into data from the fastest sensor. Third, individual sensor measurements are quantized to reduce the state space. Fourth, each merged sample is mapped to a unique state. A state database is used to hold all unique states and determine if a new state has occurred. Fifth, the data is compressed by removing repeating states. The result of the STEM algorithm is a stream of nominalized states.

For this work, the STEM algorithm was used to process heterogeneous dataset with features from multiple power system sensors. A typical logged event included 2000-3000 samples and was labeled with the name of the event. The STEM algorithm reduced each event stream to a list of ordered system states and a label. A case study was used to evaluate the performance of the STEM algorithm. Two experiments were performed. The experiments varied the quantization ranges for measured attributes to demonstrate the ability of STEM to adjust output resolution while maintaining key patterns in the data. The first experiment used a low granularity quantization while the second experiment used high granularity quantization. The average compression ratio for the two experiments was 260 and 76 for the low and high granularity quantization respectively for the entire dataset from Chapter 3. The MATLAB visualization tool was used to show patterns in the datasets were preserved by the STEM process.

The chapter is organized as follows. Section 3.2 presents Literature review. Section 3.3 presents the STEM algorithm for data size reduction keeping original patterns as a key step in data processing. Section 3.4 presents case study to apply STEM in power systems. Section 3.5 presents results from evaluation of data processing techniques followed by a discussion and conclusion in section 3.6.

3.2 Literature review

Various data processing methods are used to handle synchrophasor data. One alternative to deal with the data size would be down sampling of the data. But, this method undermines the achievement and objectives of synchrophasor technology; and also results in significant loss of information [50]. Authors in [49] used heterogeneous datasets that were randomly sample at 1 % to reduce the data size. The impact of data size reduction on classification is not discussed. Another possible shortcoming of down sampling is the tendency to loose information from sensors whose data streaming rate is very slow and event driven. Unlike PMU measurements, information such as relay trip status, breaker status, Snort network transaction logs, and control center logs are infrequent but very important to identify cyber-power events.

The open source project Hadoop has been used to handle very large synchrophasor data [56]. The MapReduce computational framework in Hadoop uses a batch based parallel approach. This method requires significant resources to parallelize the process and data storage. The Hadoop cluster installed at TVA uses 180 processor cores simultaneously for data mining and event detection. The STEM algorithm reduces

data size while maintaining critical patterns in the data. As such, STEM requires less computational and memory resources than a Hadoop based approach.

Linear Discriminant Analysis (LDA) is a supervised dimension reduction method which reduces data dimensionality by maximizing the ratio of between-class distance to within-class distance. LDA has been applied to text retrieval, face recognition, and data classification [57]. The between-class distance to within-class distance are presented in scatter matrices. A key problem with the LDA method is the scatter matrices sometimes becomes singular. PCA and Singular Value Decomposition (SVD) are used to extend the LDA method to address the singularity problem. The scalability of these LDA extensions has been an issue since these methods require the entire data matrix to be available in memory. Hence, it is difficult to apply the LDA method for large datasets such as Synchrophasor and EIDS data. Ye et al. presented a sliding window based LDA which to reduce the dimensionality of streaming data [58]. With this method data which has passed out the sliding window is forgotten. However, this method is suitable for data stream mining but not suitable for offline and batch processing methods. STEM can be used for offline, batch processing, and data stream mining methods.

Recently, Principle Component Analysis (PCA) method was used to reduce the dimensionality of synchrophasor data [50] [59] [60] [61]. PCA transforms possibly correlated variables to linearly uncorrelated variables. Dahal et al. used PCA method for data stream mining. Dimensionality reduction methods based on mutual information were studied in [50]. Xie et al. presented studies on dimensionality reduction of synchrophasor data based on PCA. Xie's method was used to develop an online early event detection system which implements dimensionality reduction at training to extract important

features from large PMU data sets [59] [60]. Among the various methods found in literature, PCA seems the most appropriate for synchrophasor data. PCA based methods are typically applied to continuous data. For the heterogeneous datasets which include both continuous and discrete data, PCA is not appropriate. Additionally, PCA is unsupervised and ignores class labels, hence PCA is not suitable for supervised classification problems especially multi-class classification problems [62]. Also, PCA is sensitive to differences in scales of input variables. Variables of different scales need preprocessing. Values should be grouped by common scale or adjusted to all have similar scales (convert from volts to kilovolts, etc.,) before using PCA. EIDS data is heterogeneous and includes continuous and discrete attribute which makes PCA inappropriate. Additionally, the STEM transformation maintains class labels and is therefore useful for supervised and unsupervised algorithms. Finally, STEM is not sensitive to scale since variables are treated independently.

3.3 State tracking and extraction method (STEM)

The STEM algorithm takes as input raw data with both continuous and discrete data format. Input to the STEM algorithm may come from separate streams connected to sensors or input may come from separate files for each input attribute or feature. STEM outputs list of states. The output can be a continuous stream of states or may be sub-lists of states associated with a particular labeled event. STEM is designed to work with streams. Logged events have artifacts across a period of time and across multiple sensors. For offline analysis, a single event includes samples from each sensor for the duration of the event. For example, typical power system events studied for this work included 20

seconds of sensor data. All samples across that period include the same label. STEM converts multiple comma separate files, with columns for each measured attribute and rows for each sample, into a single ordered list of states and a label for each event.

Algorithm: STEM

Input: Raw data from power system for the scenario of interest

Output: List of States

Step 1: Collect Raw Data. Raw data consists of measurements and time stamps. Expressions 3.1-3.3 show 3 measurements and timestamps from 2 example sensors, s1 and s2. Each sensor may measure a single item or multiple items and each sensor provides a time stamp. For example, $s1_1$ denotes the measurements from sensor s1 at timestamp 1; $s2_{a_{1.5}}$ is a measurement from sensor s2 for item 'a' at timestamp 1.5. Many instances of raw data are needed for each scenario. All sensors must have a measurement at time 0.

$$s1_1 = (s1_{a_1}, s1_{b_1}, \dots, t_{s1_1}) \tag{3.1}$$

$$s2_{1.5} = (s2_{a_{1.5}}, s2_{b_{1.5}}, \dots, t_{s2_{1.5}}) \tag{3.2}$$

$$s1_2 = (s1_{a_2}, s1_{b_2}, \dots, t_{s1_2}) \tag{3.3}$$

Step 2: Merge Raw Data. The various sensor data must be merged into a single database. Since each sensor may take measurements at different times the merged data must be time aligned. The highest frequency sensor is used as a baseline. Slower rate sensor data is merged into the baseline sensor's log file. Measurements from slower sensors which are between timestamps of the baseline sensor are delayed to the next

baseline sensor timestamp. Table 3.1 shows an example of merged raw data based on the input data from expressions 3.1-3.3.

Table 3.1 Merged raw data

Sample	Sample	Sample	Sample	Timestamp
$s1_{a_0}$	$s1_{b_0}$	$s2_{a_0}$	$s2_{a_0}$	t_{s1_0}
$s1_{a_1}$	$s1_{b_1}$	$s2_{a_0}$	$s2_{a_0}$	t_{s1_1}
$s1_{a_2}$	$s1_{b_2}$	$s2_{a_{1.5}}$	$s2_{a_{1.5}}$	t_{s1_2}

Step 3: Quantize data. Data from sensors can take many forms; real numbers, integers, Boolean values, etc. Data must be quantized to reduce state space. For sensors with real and integer values data can be quantized into numbered ranges. For example voltage and current can be quantized into low (0), medium (1), and high (2) ranges according to two thresholds r_1 and r_2. The choice of r_1 and r_2 requires expert knowledge. Expression 3.4 provides an example quantization mapping for measurements.

$$q(s_i) = \begin{cases} 0 & if\ s_i \leq r_1 \\ 1 & if\ r_1 \leq s_i < r_2 \\ 2 & if\ s_i \geq r_2 \end{cases} \tag{3.4}$$

Step 4: Map to states. A state is a set of merged and quantized sensor measurements and a time stamp. Expression 3.5 shows an example state.

$$S_j = (q(s1_i), q(s2_i), \ldots, t_i) \tag{3.5}$$

States are stored in a state database. Only unique states are stored in the database and the state index, j, is incremented for each unique state. The state database is common for all instances of all scenarios.

After mapping to states an instance of a scenarios can be represented as an uncompressed list of states. Expression 3.6 shows an uncompressed list of states representing the k^{th} instance of scenario U.

$$U_k = (S_0, S_0, S_1, S_2, \dots) \tag{3.6}$$

Step 5: Compress data into state lists. The uncompressed lists are compressed by removing sequences of states that do not change leaving just one instance of that state. This step provides a compression which reduces memory usage and results in a tuple which represents all state transitions for the system. The state transitions correspond to events. The result of compression is a list of states which represents a single instance of a scenario. A path $\mathbf{P}_i$ is a list of observed system states arranged in temporal order according to their timestamps ordered by increasing time.

$$\mathbf{P}_i = (S_0, S_1, S_2, \dots, S_n) \tag{3.7}$$

Dynamic systems will have many paths for the same scenario due to minor variations in sampled data resulting from measurement inaccuracies and changes in the larger system. For example, power systems are large interconnected systems. Changes outside the monitored portion of the power system may lead to variability in observed measurements for the same scenario in the monitored portion of the power system.

3.4 Case Study: Applying STEM for a power system with heterogeneous data sources

For the following case study the STEM algorithm was used to preprocess power system data from a diverse set of sensors. Sensors included PMU, relay logs, control panel logs, and a network monitor called SNORT. The PMU provides mostly continuous data types and the other sensors provide discrete inputs. In this section, each step of the STEM algorithm is discussed in relation to the power system case study. Results include compression ratios and MATLAB visualizations to demonstrate event patterns are maintained after applying STEM.

First an example is provided to demonstrate the STEM steps. The first step, collection of raw data is not shown. Table 3.2 shows the output of the merged raw data step. Each row in Table 3.2 is a tuple with a set of sampled attributes, a time stamp, and a label. Notice the label stay the same across many rows. This is because each scenario takes approximately 15-20 seconds which corresponds to 2000-3000 samples. In Table 3.2, the measurements are merged altogether from multiple sources and up sampled to 120 samples per seconds. In Table 3.3, the attribute values are quantized into named ranges. In Table 3.4, each instance is mapped to state ID. Table 3.4 also includes the quantized values for each attribute. This is because some algorithms prefer input in the form of individual attribute measurements, while others will take state as the input. The instances at time stamp T_0 and T_1 represent the same state of the system, hence, are represented by same state ID. In Table 3.5, the states are merged. For example, the instances from time stamp T_0 and T_1 from Table 3.4 are merged into a single instance in Table 3.5. Both compressed state IDs and compressed instances are kept in this step because compressed instances were used in NNGE and MOA in Chapter 4 and Chapter 5

respectively. Finally, Table 3.6 shows an example where each scenario is represented solely by a list of states. This example shows STEM conversion for one case of two separate scenarios, Q1 and Q2. The datasets compressed includes hundreds of cases of each scenario.

Table 3.2 Merged raw data from different sources

V	I	S	F	Z	R	E	Sn	Time	Class
135.7	253.8	0	60.01	15	0	0	0	T_0	Q1
134.2	260.1	0	59.9	14.8	0	0	0	T_1	Q1
98.2	1300	1	59.1	0.75	1	0	0	T_2	Q1
.	.	.	.	.	.	.	.	.	Q1
.	.	.	.	.	.	.	.	.	Q1
135	252.8	0	60	15	0	0	0	.	Q1
135	252.8	0	60	15	0	0	0	.	Q1
135.7	253.8	0	60.01	15	0	0	0	.	Q2
134.2	260.1	0	59.9	14.8	0	0	0	.	Q2
77.4	1500	1	60.3	1.25	1	0	1	.	Q2
.	.	.	.	.	.	.	.	.	Q2
.	.	.	.	.	.	.	.	.	Q2
135	252.8	0	60.5	15	0	0	1	T_{n-1}	Q2
135	252.8	0	60.5	15	0	0	0	T_n	Q2

Table 3.3 Quantization

V	I	S	F	Z	R	E	Sn	Time	Class
Normal	Normal	No	Normal	Normal	No	No	No	T_0	Q1
Normal	Normal	NO	Normal	Normal	No	No	No	T_1	Q1
Low	High	Yes	Low	Zone 1	Yes	No	No	T_2	Q1
.	.	.	.	.	.	.	.	.	Q1
.	.	.	.	.	.	.	.	.	Q1
Normal	Normal	No	Normal	Normal	No	No	No	.	Q1
Normal	Normal	No	Normal	Normal	No	No	No	.	Q1
Normal	Normal	No	Normal	Normal	No	No	No	.	Q2
Normal	Normal	No	Normal	Normal	No	No	No	.	Q2
Low	High	Yes	Low	Zone 1	Yes	No	Yes	.	Q2
.	.	.	.	.	.	.	.	.	Q2
.	.	.	.	.	.	.	.	.	Q2
Normal	Normal	No	Normal	Normal	No	No	No	T_{n-1}	Q2
Normal	Normal	No	Normal	Normal	No	No	No	T_n	Q2

Table 3.4 Mapped to state ID

V	I	S	F	Z	R	E	Sn	State	Class
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q1
Normal	Normal	NO	Normal	Normal	No	No	No	S_0	Q1
Low	High	Yes	Low	Zone 1	Yes	No	No	S_1	Q1
.	.	.	.	.	.	.	.	S_2	Q1
.	.	.	.	.	.	.	.	.	Q1
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q1
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q2
Low	High	Yes	Low	Zone 1	Yes	No	Yes	S_4	Q2
Low	High	Yes	Low	Zone 1	Yes	No	Yes	S_4	Q2
.	.	.	.	.	.	.	.	S_5	Q2
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q2

Table 3.5 Compressed states

V	I	S	F	Z	R	E	Sn	State	Class
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q1
Low	High	Yes	Low	Zone 1	Yes	No	No	S_1	Q1
.	.	.	.	.	.	.	.	S_2	Q1
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q1
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q2
Low	High	Yes	Low	Zone 1	Yes	No	Yes	S_4	Q2
.	.	.	.	.	.	.	.	S_5	Q2
Normal	Normal	No	Normal	Normal	No	No	No	S_0	Q2

Table 3.6 State lists

State list	Class Label
$S_0, S_1\ S_2\ S_3$ .. S_m	Q1
$S_0, S_1\ S_4\ S_6$.. S_k	Q2
……	……..
$S_1\ S_8\ S_9$.. S_l	Qo

3.4.1 Collect raw data

A PMU provides measurements of different electrical quantities as shown in Table 3.7 in numeric format. For this case study, each PMU provided 27 measurements. There are four PMUs.

Table 3.7 Measurements from PMU, relay logs, control panel logs, and SNORT

Measurements	Source	Number of measurements	Data Type
PMU Timestamp	PMU	1	Continuous
Voltage Phase angles Phase A, B, C	PMU	3 x 4 = 12	Continuous
Voltage Magnitude Phase A, B, C	PMU	3 x 4 = 12	Continuous
Current Phase angle Phase A, B, C	PMU	3 x 4 = 12	Continuous
Current Magnitude Phase A, B, C	PMU	3 x 4 = 12	Continuous
Voltage Sequence angles Zero, Positive, Negative	PMU	3 x 4 = 12	Continuous
Voltage Sequence Magnitude Zero, Positive, Negative	PMU	3 x 4 = 12	Continuous
Current Sequence angles Zero, Positive, Negative	PMU	3 x 4 = 12	Continuous
Current Sequence Magnitude Zero, Positive, Negative	PMU	3 x 4 = 12	Continuous
Frequency	PMU	1 x 4 = 4	Continuous
Rate of change of frequency	PMU	1 x 4 = 4	Continuous
Apparent impedance	Calculation	1 x 4 = 4	Continuous
Breaker Status	Relay Log	1 x 4 = 4	Discrete
Operator Remote Trip	Control Panel	1 x 4 = 4	Discrete
Detect Remote Trip Network Packet	SNORT	1 x 4 = 4	Discrete

Figures 3.1-3.3 show screenshots of actual PMU measurements and relay event logs obtained from the test bed. Figure 3.1 and 3.2 are taken from the OpenPDC user interface. Figure 3.3 is a relay event log from the GE Entervista software used to monitor and control relays.

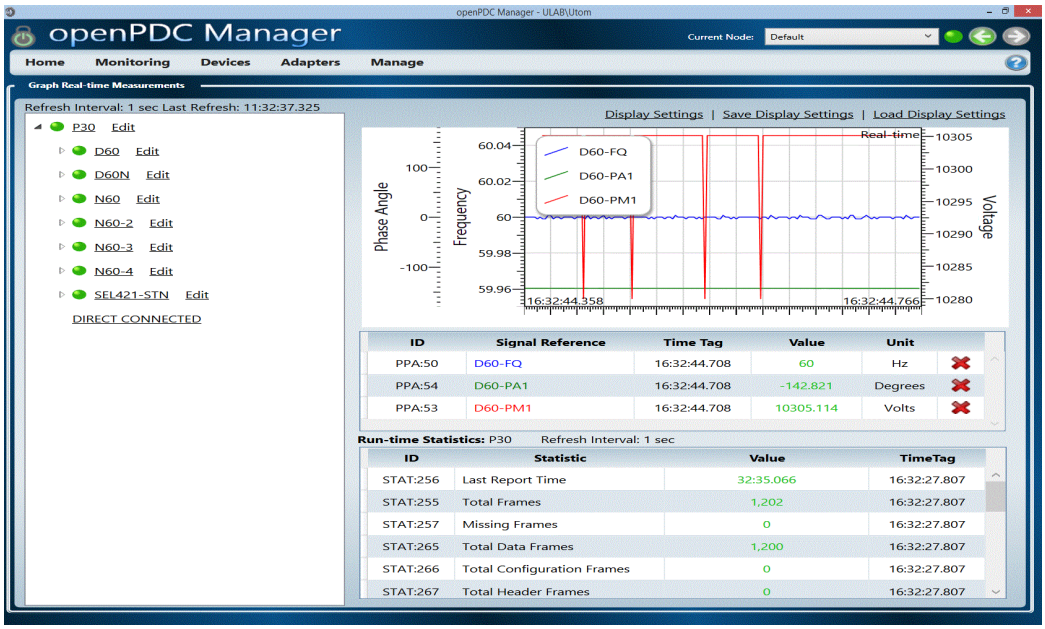


Figure 3.1 OpenPDC screenshot showing actual PMUs in the test bed

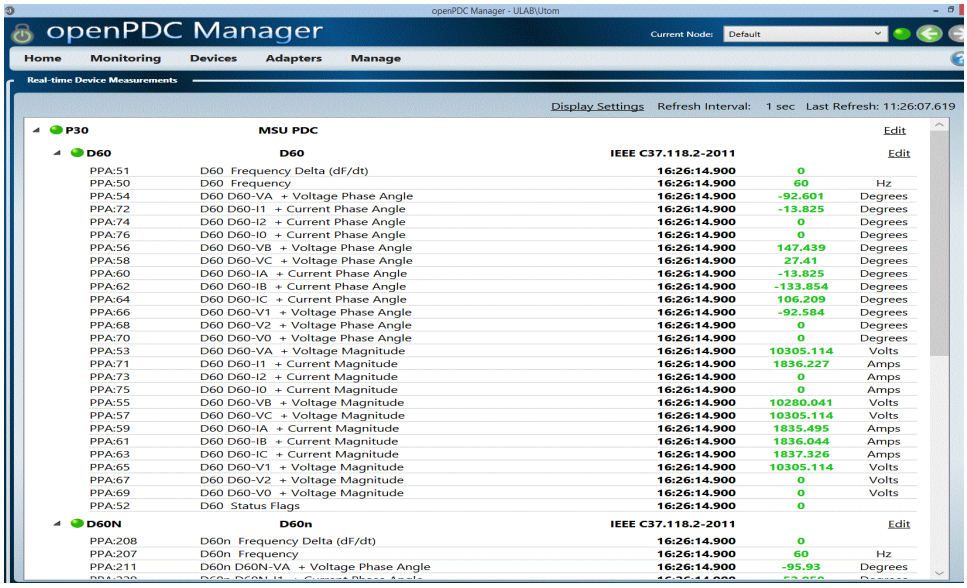


Figure 3.2 Actual measurements from GE D60

```
FORMAT,SHORT_EVENT,Event Number,Date/Time,Cause (Hex),Cause
FORMAT,SNAPSHOT_EVENT,Event Number,Date/Time,Cause (Hex),Cause
SHORT_EVENT,1,Jan 24 2014 22:53:52.517192,003E0000,EVENTS CLEARED
SHORT_EVENT,2,Jan 24 2014 23:01:29.051450,80080151,RESET OP(COMMS)
SHORT_EVENT,3,Jan 24 2014 23:03:08.641253,800800AD,GND DIST Z2 PKP A
SHORT_EVENT,4,Jan 24 2014 23:03:09.040699,801400AD,GND DIST Z2 OP A
SHORT_EVENT,5,Jan 24 2014 23:03:09.040699,8000034A,TRIPBUS 1 PKP
SHORT_EVENT,6,Jan 24 2014 23:03:09.040699,8004034A,TRIPBUS 1 OP
SHORT_EVENT,7,Jan 24 2014 23:03:09.040699,003E0001,OSCILLOGRAPHY TRIG'D
SHORT_EVENT,8,Jan 24 2014 23:03:09.040699,00080001,TRIP-LINE    On
SHORT_EVENT,9,Jan 24 2014 23:03:09.109356,802400AD,GND DIST Z2 DPO A
SHORT_EVENT,10,Jan 24 2014 23:03:09.130162,00090001,TRIP-LINE    Off
SHORT_EVENT,11,Jan 24 2014 23:03:11.041857,00060007,H2C          On
SHORT_EVENT,12,Jan 24 2014 23:03:11.041857,00080002,CLOSE-LINE   On
SHORT_EVENT,13,Jan 24 2014 23:03:17.042743,00070007,H2C          Off
SHORT_EVENT,14,Jan 24 2014 23:03:17.042743,00090002,CLOSE-LINE   Off
```

Figure 3.3 Actual relay events with time stamps

3.4.2 Merge raw data

The measurement data from the PMU, relay logs, Snort logs, and Control panel logs were merged into a single file. The PMU measurements were measured at 120 samples per second. The apparent impedance seen by relay was calculated by using PMU measurements at relay terminal [63]. Relay status, Snort logs, and Control panel logs are asynchronous. To merge the PMU measurements was chosen as a reference and the relay logs, Snort logs, and Control panel logs were up sampled prior to merging.

3.4.3 Quantization

Power systems are dynamic and the measurements from them system continuously change even while the system is in a normal operating state due to change in loads and other switching. State tracking is difficult for continuous raw data. To facilitate proper state tracking, measurements with large state space should be quantized in such a way that the quantization interval maintains important patterns in the data. The

deviation of these measurements from normal state depends upon the type of event. For example, during faults, current values for the faulted phase swing over a very large range and the voltage dips significantly. Also, the frequency of the system and impedance of the line change significantly. For transmission line and generator loss, frequency excursion is significant but voltage and current values do not change as much when compared to faulted scenarios. If changes in the measurements are large, even large quantization intervals can capture the event pattern but if the measurements change within the narrow range, smaller and more quantization intervals are necessary. So, domain expert knowledge is needed to create proper quantization intervals. Quantization depends upon the type of system and the desired goals of the EIDS. For the EIDS in this case study, it is necessary to distinguish power system disturbance events from cyber-attacks which mimic these same events.

In this study, each measurement was split into multiple quantization intervals. The quantization interval of each measurement is shown in the Table 3.8. Table 3.8 includes the name of the attribute, the name of each quantization interval, the enumeration used by the learner, and the range for each interval. For example, normal range of voltage is assumed to be between 0.95 and 1.05 PU. Below 0.95 PU is assumed to be low voltage and above 1.05 PU is assumed to be high voltage which is an abnormal condition. For the current values, over current protection setting guidelines are used for basic quantization [64]. The majority of events in this study are related to power system faults, so, voltage and current measurements swing over a wide range.

Table 3.8 Measurement quantization

Data attribute	Quantization Interval Name	Quantization Interval Enumeration	Range
Voltage	Low, Normal, High	{0, 1, 2}	(0-0.95), [0.95-1.05), [1.05-∞)
Voltage relative angle	Low, Normal, High	{0, 1, 2}	[(LT- Upper threshold (UT)), [LT- Upper threshold (UT)), [UT- ∞)
Current	Low, Normal, Warning, High	{0, 1, 2, 3}	(0- Lower Threshold (LT)), [LT- 2 ×Maximum load current (MLC)), [2 ×MLC- Prefault current), [Prefault current - ∞]
Frequency	Low, Normal, High	{0, 1, 2}	(0-59.8 Hz), [59.8-60.2 Hz), [60.2- ∞]
Impedance	Zone 1, Zone 2, Normal	{0, 1, 2}	(0-0.80 PU), [0.80-1.5), [1.5-∞]
Positive Sequence	Yes, No	{1, 0}	{non-zero, 0}
Negative Sequence	Yes, No	{1, 0}	{non-zero, 0}
Zero Sequence	Yes, No	{1, 0}	{non-zero, 0}
Relay logs	Trip, No trip	{1, 0}	{1, 0}
Control panel logs	Scheduled maintenance, No schedule maintenance	{1, 0}	{1, 0}
SNORT	Network transaction, No network transaction	{1, 0}	{1, 0}

Frequency quantization is more complex. Choosing the quantization interval depends upon the interconnections and the type of control schemes. In the eastern interconnection under frequency load shedding starts at a threshold of 59.7 Hz. In ERCOT two frequency thresholds are used for load shedding. Load shedding 59.8 Hz and

at 59.7 Hz a second group of loads are defined shed [65]. For this study, 59.8 Hz was used as the threshold to define low frequency. No information was found on a high threshold. Therefore, high frequency was classified as above 60.2 Hz.

The voltage relative angle is useful to detect power system stress. Developing quantization ranges for voltage relative angle requires significant study and depends upon many factors including distance between buses, amount of power transfer, and physical characteristics of the network [1]. For a given reference angle, there will be a voltage relative angle for all other PMUs. Each voltage relative angle will have a unique quantization range. For this work, voltage relative angle is not used. Apparent impedance is categorized based on distance protection zone boundaries settings [64]. The apparent impedance significantly changes during faults, the zone boundaries can be used to define quantization intervals. This work used two distance zone protection. A quantization interval was created for each zone and a third interval defines the normal apparent impedance. Voltage and current sequence components can be used to identify faults in the systems. In this study, sequence components where quantized into zero and non-zero intervals. The zero range represents the no fault case and the non-zero case occurs during a fault. Different combinations of sequence components take the non-zero range for different types of faults. The relay logs, control panel logs, and SNORT log entries are event driven. Each has only binary values as they are used to identify whether a particular change occurred or not.

Once quantization is completed, the raw data transforms from raw data to nominal data. The transformation of data into a nominal format with a reduced state space is suitable for various machine learning, data mining, and pattern discovery methods.

3.4.4 State mapping and compression

Once each row of the dataset is quantized, each row is mapped to a state ID. Unique states are provided an ID and repeated states use the same ID as previous instances of that state. For the case study, each cyber-power event has 2000-3000 instances (rows). After mapping each row will have an assigned state ID. Compression removes repeated states in a sequence. After compression each event is represented by a temporally ordered list of states and a label.

After each row is assigned with state ID, in the next step, STEM sequentially captures only distinct states, compress states, and stores it in the database. In this way the data size is significantly reduced by intelligently pruning the repetitive states.

3.5 Results: Evaluation of STEM algorithm

This section presents the evaluation of STEM algorithm if it preserves the original pattern in the datasets. The results show the compression technique reduces the size of data significantly and retains events and patterns very well. Also, the results show that the variation in the quantization interval significantly changes the number of compressed states, data size, and fidelity of the attributes.

3.5.1 Experiment 1

The objective of this experiment was to demonstrate the ability of the STEM algorithm to compress data while maintaining key events (patterns) and to reduce the data size. The analysis of scenario cases presented here were obtained from dataset described in Chapter 2. The two generator three bus system with two transmission lines and one dynamic load was used to create the datasets. The transmission lines are protected with

four distance protection relays and power system measurements were obtained from four PMUs.

In this experiment, the attributes are quantized using the quantization intervals in table 3.8. For this experiment, the scenario used was a SLG fault. The transmission line is protected by relays R1 and R2. The fault was simulated on 85% of the line from the perspective of relay R1. So, the fault falls within zone 2 of R1 and zone R2. Thus, R1 operates with a time delay and R2 operates instantaneously. Both relays use an auto-reclosing scheme. The current and voltage plots shown for this experiment were measured by a PMU embedded in R1. Although, current and voltage were plotted for only PMU1, in the actual dataset there is data from three additional PMUs.

MATLAB was used to provide ribbon plots showing current and voltage behavior before and after STEM compression. Figure 3.4, Figure 3.5, and Figure 3.6 show the three phase current plotted for raw, quantized, and compressed form. The X-axis presents the instance number, the Y-axis presents the attribute number (phase A, B, and C are attribute 1, 2, and 3 respectively), and the Z-axis presents the current measurements. In Figure 3.4, several events are noticeable in raw data. When the SLG fault occurs on phase A, the phase A current goes from around 200A to 1500A. Next, the relays trip and open their breakers which causes the current to go to zero. After a fixed time interval the relays reclose and the phase A current shows a small transient before finally returning to a normal current value. Phase B and Phase C were also affected by the fault. Three pole tripping and reclosing opens and closes all three lines.

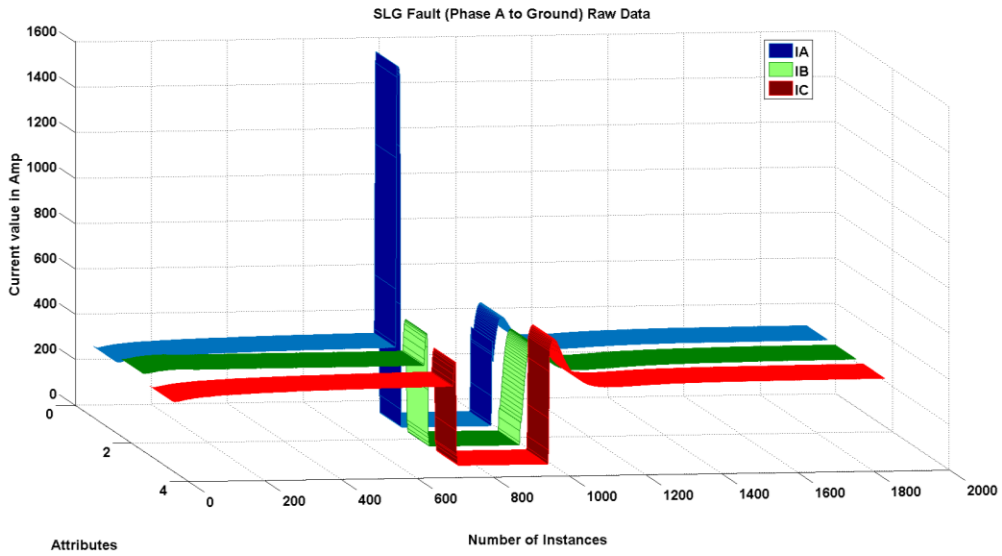


Figure 3.4 Three phase current measurements from relay R1

Figure 3.5 shows the current after quantization. The magnitude of the current values are quantized into four intervals. {Low, Normal, Warning, and High} which are mapped to {0, 1, 2, 3} respectively and is shown in Figure 3.5. The key events in the data are still present. The large jump in phase A current is still present. The small transients on phase B and phase C are lost because the quantization intervals were not designed to catch small transients. Smaller transients can be maintained by making smaller quantization intervals. But for event classification presented in Chapters 4 and 5 this quantization is acceptable because it keeps the key events in the data required for classification.

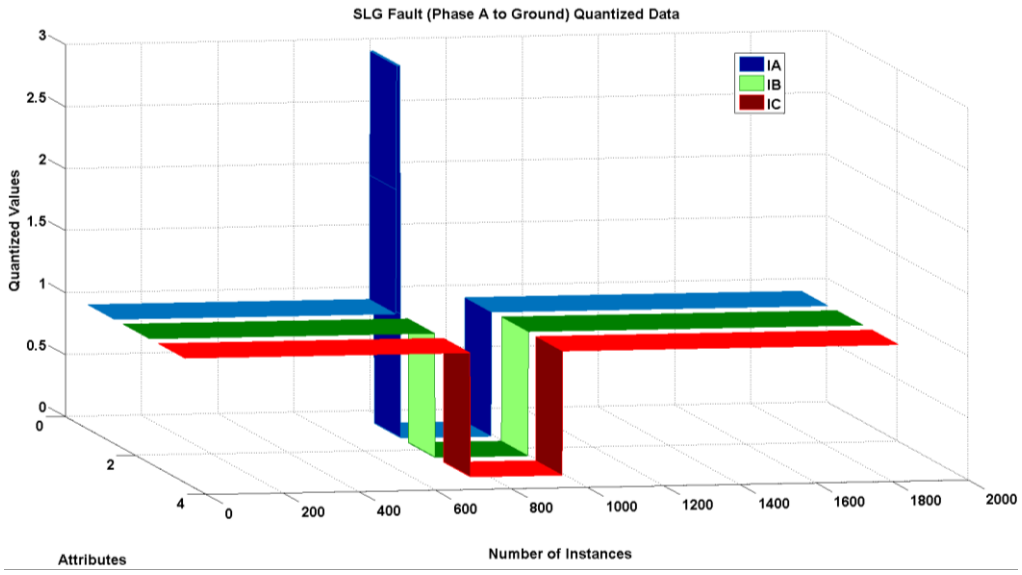


Figure 3.5 Three phase quantized current measurements

Finally, Figure 3.6 shows compressed data. Figure 3.3 still shows a large increase in phase A current. The number of samples in Figure 3.6 is reduced from 2000 to 35 which is a significant reduction.

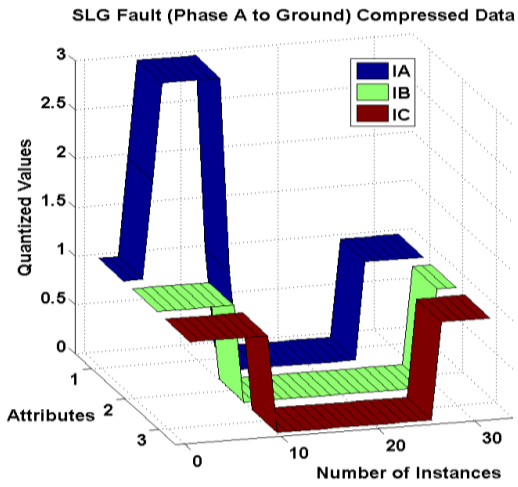


Figure 3.6 Three phase compressed current measurements

Figure 3.7 shows raw three phase voltage measurements for the same scenario. During the SLG fault on phase A, the phase A voltage dips significantly and recovers, with small transients, to normal as soon as relay clears the fault. The voltage dips momentarily during reclosing and eventually settles to a normal voltage. Phase B and C voltages also experience slight changes during the fault and reclosing. Figure 3.8 shows post quantization. All key events are maintained. Quantization picks up slight dip on phase B and C voltage because both go below 0.95 PU. The voltage changes in only two category of normal and low. The compression plot in Figure 3.9 shows reduction in numbers of samples from 2000 to 35 but retains key events in the data.

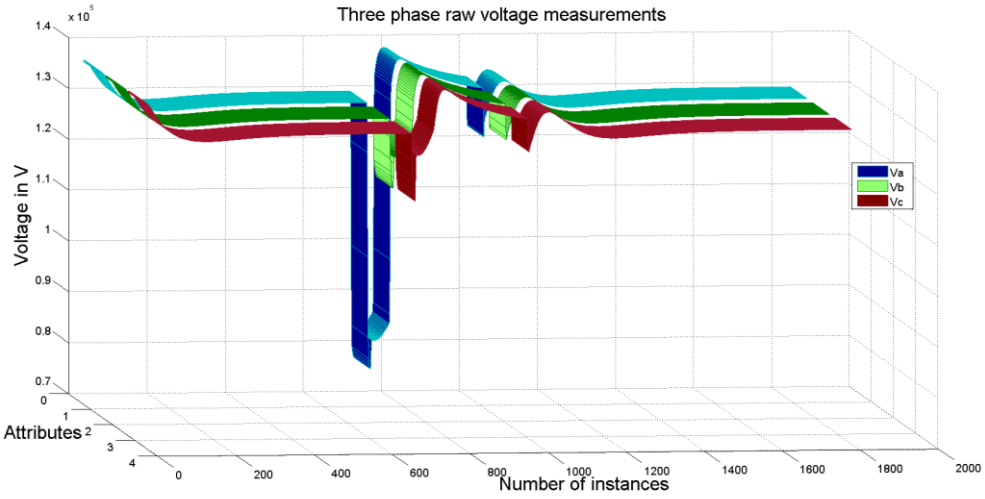


Figure 3.7 Three phase voltage raw measurements from relay R1

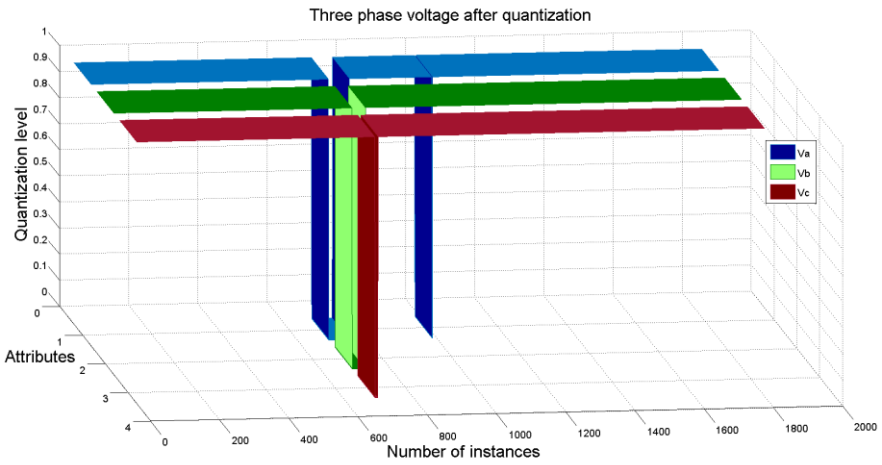


Figure 3.8 Three phase quantized voltage measurements

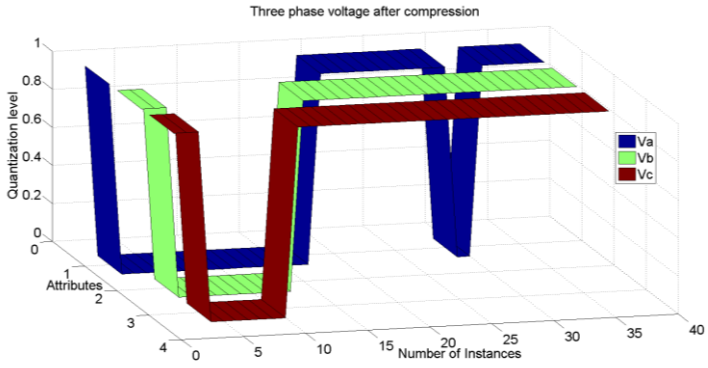


Figure 3.9 Three phase compressed voltage

Figure 3.10 shows the data logs from other sources, relay logs, control panel logs, and the Snort network monitor, for the same scenario. The sensors for all three types of data provide binary information. For relay logs they binary states indicate whether the relay is tripped (value 1 in the graph) and relay is not tripped (0 in the graph). Because the data from the sensor is already binary the raw and quantized data are the same. Since, the event is SLG fault on a line and the relays operate as expected, relays R1 and R2

show the presence of a trip signal. As the fault is at 85% of the line, R1 (blue) operated with a time delay while relay R2 (red) operated instantly. This relationship was maintained in the compressed data, as shown in Figure 3.11, although the number of samples were significantly reduced.

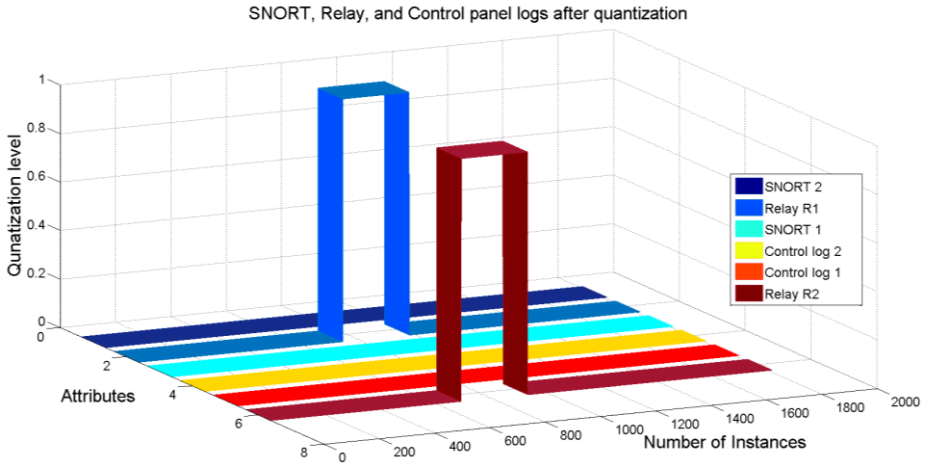


Figure 3.10 Data logs from relays, control panel, and SNORT

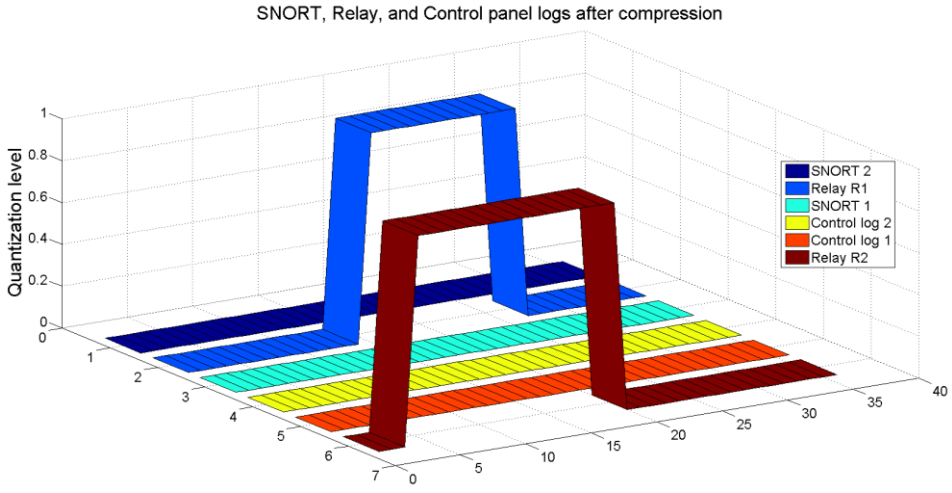


Figure 3.11 Compressed data logs

In conclusion, the STEM algorithm captures all of the key events needed for event classification.

The analysis for Figures 3.4 -3.11 was performed for only one case among 10,237 cases in the dataset. The STEM algorithm was used to process all 10,237 cases of scenarios in the *Dataset 1* to demonstrate the compression ratio. The size of *Dataset 1* is 11.638 gigabyte (GB) and includes three phase voltages, three phase currents, apparent impedance, and frequency from all four PMUs and logs from all sources. Table 3.9 shows an example of data compression ratio. In this study, compression ratio CR_1 was defined as the ratio of merged raw data size from Table 3.2 to the compressed state data size from Table 3.5. Compression ratio CR_2 was defined as the ratio of merged raw data size from Table 3.2 to the state lists from Table 3.6. Table 3.9 shows compression ratio by the type of scenario. Raw and compressed data of one example case of each scenario is shown in the table. Also CR_1 for combined *dataset 1* is shown in the table.

Different scenarios have different compression ratios because different scenarios have different numbers of events. If a scenarios represents a significant change in dynamics of the system, then the system goes through sequence of many state changes. In contrast, if a scenario does not change much from its normal operating range, it will have less states. Hence, the compressed data has variable data size for different scenarios. In addition, the size of raw data changes if the scenario run time changes which results in different data sizes.

The total size of all state lists for all cases in Dataset *1* is 2921 kilobytes (KB) when saved as a comma separated file. The compression ratio CR_2 is 4178. The large compression ratio shows the final output of STEM algorithms is greatly compressed and

very useful for batch processing data mining techniques which require all data to be present in the memory when training and testing.

Table 3.9 Comparison of compression ratio

Data associated with on example case of each scenario	Raw data size	Compressed data size	Compression ratio CR_1
SLG fault (S1)	776 KB	6 KB	130
Fault replay (S2)	1256 KB	6 KB	209
Line maintenance (S3)	918 KB	4 KB	229
Command injection to one relay (S4)	941 KB	5 KB	188
Command injection to two relays (S5)	927 KB	4 KB	232
Single relay disabled attack and fault (S6)	1124 KB	6 KB	187
Single relay disabled and line maintenance (S7)	824 KB	6 KB	137
Two relay disabled and line maintenance (S8)	920 KB	2 KB	460
Normal operation (S9)	2630 KB	3 KB	877
Dataset 1 (S10)	11.638 GB	45.7 MB	260

3.5.2 Experiment 2

The objective of this experiment is to evaluate the impact of quantization interval changes. The same SLG fault scenario from experiment 1 was used for this experiment. The number of quantization intervals for current values was increased from 4 to 33 which equates to 50 Ampere current intervals. Also, the number of quantization intervals for voltage was increased from 3 to 15 where the intervals were evenly distributed across the range. The quantization intervals for all other attributes was kept same as in the first experiment. Figure 3.12 and Figure 3.13 show quantized and compressed three phase current plots. Unlike experiment 1, the small transients during the fault and at reclosing

are present after quantization and compression. All other key events are also still present after quantization and compression. This shows that STEM is able to be tuned to capture events of different sizes.

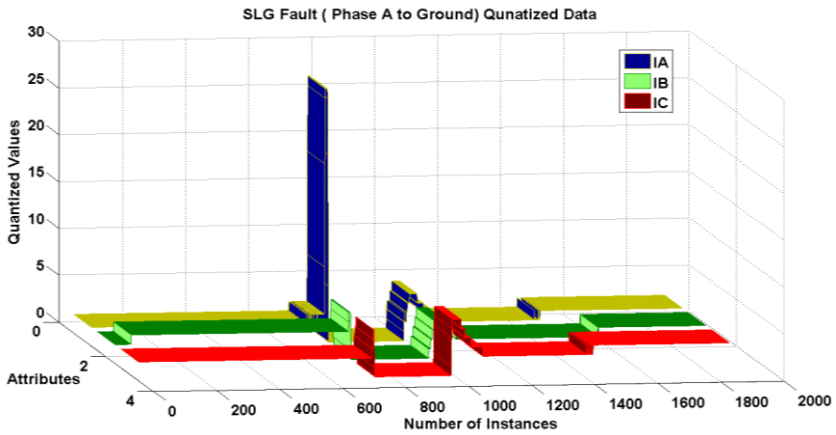


Figure 3.12 Quantized current with smaller quantization interval

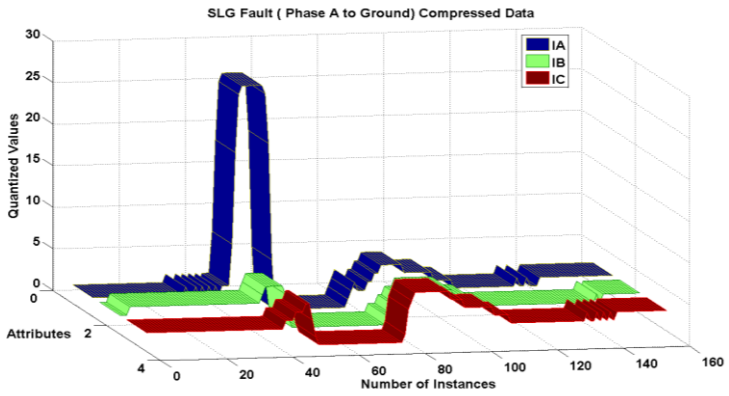


Figure 3.13 Compressed current with smaller quantization intervals

Figure 3.14 and Figure 3.15 show three phase voltage measurements. Again, smaller quantization intervals result in the shape of the quantized plot being closer to the

raw measurement plot. The average compression ratio CR_1 for all cases in *Dataset 1* decreased as shown in Table 3.10. The total CR_1 ratio decreased from 260 to 55. Hence, it can be concluded that STEM can be tuned to adjust fidelity to the original signal at the expense of compression ratio. Additionally, the user has the flexibility to adjust quantization intervals of individual measurements.

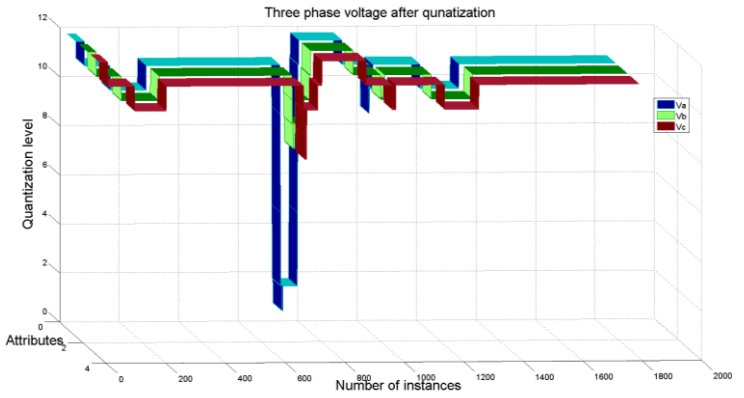


Figure 3.14 Quantized voltage with smaller quantization intervals

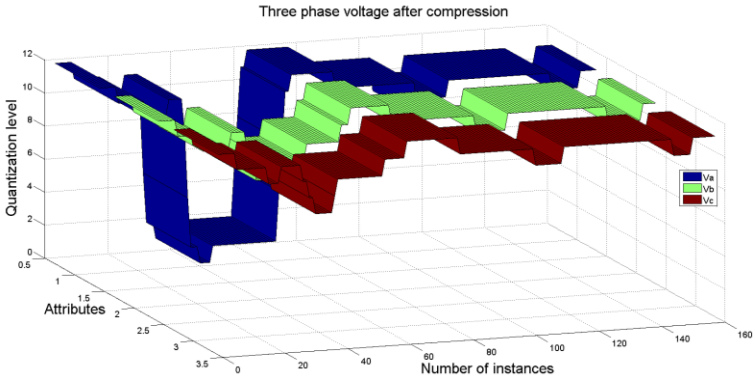


Figure 3.15 Compressed voltage with smaller quantization intervals

The smaller quantization intervals results more states in the final STEM output for each scenario. The number of states increased from 35 to 160 from experiment 1 to experiment 2. The size of all state lists derived from *Dataset 1* for this experiment is 7796 Kilobytes (KB). As such, compression ratio CR_2 decreased from 4178 to 1564. The increase in the number of quantization intervals had a significant effect on the compression ratios. However, the size of STEM output data is still suitable for data mining algorithms which are sensitive to memory resource constraints.

Table 3.10 Comparison of compression ratio

Data associated with on example case of each scenario	Raw data size	Compressed data size	Compression ratio CR_1
SLG fault (S1)	776 KB	22 KB	35
Fault replay (S2)	1256 KB	11 KB	114
Line maintenance (S3)	918 KB	34 KB	27
Command injection to one relay (S4)	941 KB	23 KB	41
Command injection to two relays (S5)	927 KB	14 KB	66
Single relay disabled attack and fault (S6)	1124 KB	16 KB	70
Single relay disabled and line maintenance (S7)	824 KB	41 KB	20
Two relay disabled and line maintenance (S8)	920 KB	4 KB	230
Normal operation (S9)	2630 KB	58 KB	45
Dataset 1 (S10)	11.638 GB	215 MB	55

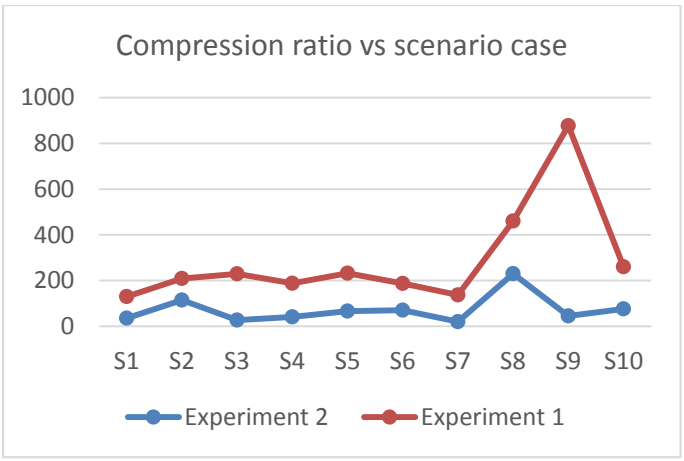


Figure 3.16 Compression ratio for different scenario cases

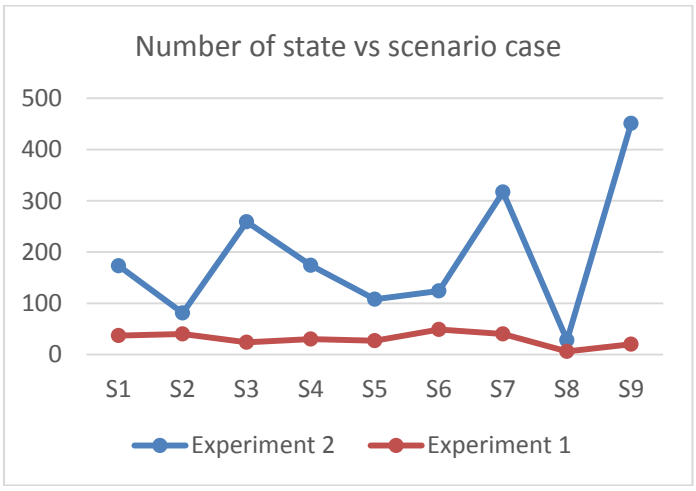


Figure 3.17 Number of states for different scenario cases

Figure 3.16 shows a comparison of compression ratio CR_1 between experiment 1 and experiment 2. The normal operation scenario (S9) has a significant change on the CR_1 compression ratio. This change is due to constantly changing loads which lead to changes in current and voltage measurements which are picked by the small quantization

intervals and results in more states. Figure 3.17 shows the number of states in different scenarios in experiment 1 and experiment 2. Normal operation (S9) has 451 states.

3.6 Conclusion

WAMS heterogeneous data represents big data with high volume, velocity, and variety and poses significant resource challenges when used with traditional batch processing data mining methods. Traditional batch processing methods require all data to be loaded in memory before building a training model and testing the training model. Hence, large WAMS heterogeneous data in size of terabytes does not fit into memory. So, appropriate data processing techniques are required to reduce the size in such a way that key patterns in the data are sustained and be useful for data mining pattern matching studies. In this chapter, a state tracking and extraction method (STEM) for heterogeneous datasets was developed to address the data size problem. STEM is useful to reduce the size of the data while maintaining key patterns in the dataset. The size, patterns, and number of states in the reduced data depends upon three variables, number of attributes, quantization intervals, and time window, in STEM. The STEM variables directly impact the size, pattern, and number of states in the reduced dataset.

Since STEM keeps class labels throughout the process, data required for data mining techniques are available at any step of the process. As the performance of data mining techniques heavily depends on input data, data processing plays an important role and algorithms can take advantage of data transformations at any step of the algorithm. Data from different steps of STEM algorithm was used in evaluating NNGE and HAT in Chapter 4 and Chapter 5.

CHAPTER IV

APPLYING THE NNGE ALGORITHM FOR CYBER-POWER EVENT CLASSIFICATION

4.1 Introduction

Timely and appropriate responses during power system disturbances and abnormal conditions heavily depend on situational awareness. Quick and informed responses have significant impacts on system reliability and security [1]. Current practices for power system event detection are insufficient to identify a wide variety of natural disturbances and cyber-attacks. These natural events and cyber-attacks can impact small regions and also create cascading failures and affect large areas if not detected and isolated properly. Data obtained from synchrophasor based Wide Area Measurement Systems (WAMS) can be combined with other asynchronous data sources to create event and intrusion detection systems (EIDS) to classify cyber-power events. An EIDS is a system that detects and classifies power system and cyber-attacks with high accuracy, low false positive rate and classification time, and requires low memory usage. This work introduces a novel methodology to create an effective EIDS using a state of the art data mining algorithm called Non-Nested Generalized Exemplars (NNGE) with input data preprocessed using the STEM algorithm presented in Chapter 3. Evaluation of NNGE with STEM resulted in classification accuracy of more than 90%, false positive rate with

less than 5%, and classification time much faster than the current synchrophasor data rate and low memory usage.

Data mining is a useful tool to analyze power system data to discover patterns. Machine learning algorithms including Artificial Neural Networks (ANN) [17] [18], Decision Trees (DT) [13] [14], and rule based classifiers have been extensively used in power system applications [66]. One of the shortcomings of classical batch processing is that the data needs to be in memory to train the model. These algorithms may require more memory than available. Hence, batch processing algorithms do not scale well if the dataset is very large [67] such as is the case with power system WAMS data. However, the STEM algorithm can be used to preprocess power system WAMS data to reduce data size while maintaining critical patterns. Using raw WAMS data without preprocessing can cause rules or decision trees created to grow significantly especially in the case of a multi-class classification problem. The large number of rules can be memory intensive and consequently require more time to classify events. In the case of WAMS, where the volume, velocity, and variety of datasets are high, the classifier must have the capability to generalize rules and decision trees in such a way that it does not suffer from poor accuracy, slow speed, and memory issues. The requirements for effective EIDS is summarized in the Table 4.1.

Table 4.1 EIDS requirements

Index	Requirements description
1	The EIDS should be able to detect or classify a wide variety of power system faults, disturbances, control actions, and cyber- attacks.
2	Classification with greater than 90% accuracy.
3	Classification with less than 5% false positives.
4	Classification faster than synchrophasor data rate.
5	The EIDS should be able to handle large volume WAMS heterogeneous datasets.
6	Minimal memory usage.

For this work, the NNGE data mining algorithm was chosen because NNGE with STEM fulfills the above mentioned requirements. NNGE is a nearest-neighbor-like algorithm based on generalized exemplars stored in memory. A nearest neighbor learner uses distance between a new example and a set of exemplars in memory to make a decision whether the new example belongs to a particular class. Generalized exemplars are a set of examples that represent one or more examples in the training datasets and generalized exemplars are represented by a hyper-rectangle. Nearest-neighbor-like NNGE uses a hybrid approach that combines the concept of a distance function and rules. The combination of these two methods provide better classification performance than only using instance based learning or rule induction methods. Generalization of exemplars reduces classification time without sacrificing accuracy [68]. In addition, the ability of NNGE to classify multiclass scenarios, sequential data, and handle different data formats such as numeric, nominal, and missing attributes makes NNGE a suitable method to develop a cyber-power EIDS [68].

In this chapter, the impact of the STEM data processing algorithm on the classification accuracy of the NNGE algorithm was evaluated. Second, NNGE was

evaluated for suitability for cyber-power event classification to create EIDS. Classification results support this hypothesis as the classification accuracy for both multiclass and binary class experiments were above 90%.

The remainder of the chapter is organized as follows. Section 4.2 presents the literature review. Section 4.3 presents NNGE algorithm for training and testing classifier. Section 4.4 presents implementation of NNGE with STEM for EIDS and section 4.5 presents experiments with results followed by conclusions in section 4.6.

4.2 Literature review

Current research on applying data mining to synchrophasor data for power system fault and disturbance classification can be found in [69] and [34]. The K-nearest neighbor algorithm was used to classify three phase faults (3LG), voltage oscillation, and voltage sag scenarios in [69]. The algorithm accuracy is not provided in [69]. Hoeffding Tree based stream data mining is used in [34]. This approach was able to classify 3LG and single line to ground (SLG) faults grouped for binary classification with greater than 90% accuracy. Both [69] and [34] used simulated power system data. Both [69] and [34] propose methods to mine synchrophasor data. However, both are designed for power system measurement data only and do not incorporate any other types of system information. By only considering measurement data it is impossible to detect cyber-attacks such as fault replay or command injection attacks in which valid measurements or control commands are replayed.

Classification and regression trees (CART) have been used to detect impending island formation in [35]. Similarly, decision trees (DT) have been used to study

oscillatory and voltage stability events. Additionally, a dynamic security assessment was performed using ensemble based DTs [36] [37]. Reference [70] [71] studied various clustering techniques to identify appropriate unsupervised learning methods to identify a number of events in utility provided datasets. In these works, only specific cases of power systems conditions are considered and cyber-attack induced events are not considered. Only limited synchrophasor measurements were considered in [70] [71] and heterogeneous data was not used.

The emergence of the smart grid, which depends heavily on communication infrastructure, has provided many benefits, but, also has introduced many vulnerabilities in power systems. Many researchers have worked on different intrusion detection systems (IDS). Network based IDS monitor network traffic to search for artifacts of cyber-attacks. Yang et al. propose an IDS to detect man in the middle (MITM) and denial of service (DoS) attacks [72]. Zhang et al used a data mining approach to identify malicious data and possible cyber-attacks from communication traffic from different levels of networks [73]. Researchers in [74] proposed anomaly detection techniques which extract behaviors from various communication protocols to create a full description of the communication pattern in an industrial control system. Network based IDS are able to detect malicious network traffic, however, they cannot detect physical changes in a system from cyber-attacks. Specification based IDS monitor system state and alert when the state approaches an unsafe or disallowed state. A specification based IDS for advanced metering infrastructure (AMI) tracked system state using a manually built state machine is presented in [75]. The AMI specification based IDS works in concept, but, does not scale well due to the required manual construction of a state machines to track bulk electric

transmission system state. A few IDS described in literature leverage power system theories. Optimal power flow [76], and weighted state estimation [77] methods are used to detect cyber-attacks and false data injection attacks. However, these methods are only applicable to very limited cyber-attacks and cannot detect a wide variety of scenarios.

Nearest neighbor approaches have been explored by other researchers. Researchers at Tennessee Valley Authority (TVA) implemented instance based learning to train Hadoop to identify patterns in synchrophasor data [56]. In this case, a combination of SAX and Euclidian distance functions were used to analyze the closeness of the archived synchrophasor data to train samples for un-damped oscillation, sudden load shed, and islanding. This work demonstrated the ability of an algorithm to identify patterns in data, however, only limited scenarios were considered. In addition, this work does not consider the use of heterogeneous data and cyber-attack events for classification. The TVA method also does not consider the sequential nature of power system events.

NNGE has been tested using various data types and sizes to evaluate the performance in terms of classification accuracy and speed [68]. Datasets used for NNGE evaluations consist of a wide variety of data types including continuous, nominal, Boolean, and numeric. These datasets can be obtained from the UCI repository [5]. NNGE has been used to test data that are sequential in nature. NNGE was applied to Breast Cancer-Wisconsin (BCW) datasets where samples arrive periodically in a chronologically ordered dataset. Similarly, NNGE was applied to datasets with E. coli promoter gene sequences. The accuracy for BCW and E. coli datasets using NNGE were 95.4 % and 78% [68].

In recent research, a fusion of synchrophasor data with device and system logs with time synchronization was used to explore the viability of using machine learning methods to detect power system and cyber-attack events [49]. One percent sampled raw heterogeneous data with minimal processing was used to test various data mining algorithms. The test results showed variable classification accuracy across tested algorithms. These experiments were performed without considering the ability of algorithms to handle the sequential nature of heterogeneous data. The NNGE method was one of the algorithms used in the study. However the performance of NNGE was very poor for this work. This work attempted to classify individual rows found in datasets which contained thousands of temporally ordered samples related to a single event. Such an approach does not consider the pattern of behavior related to the event. For this dissertation, the STEM algorithm was used to preprocess data for NNGE. STEM provides an ordered list of states related to one event. Each event is handled in its entirety rather than considered piecemeal.

Pan et al. presented common path mining to create an IDS which used heterogeneous data to create a hybrid intrusion detection system capable of classifying cyber-attacks and power system events [38]. Common path mining used the STEM algorithm to preprocess data and then used frequent item set mining to extract common paths associated with specific system behaviors. A common path is a temporally ordered list of critical states associated with a specific cyber-attack or power system event type. Common paths were used as signatures for classification. The algorithm performed well. The common path mining evaluation shows some cases in which observed behavior matched multiple event common paths associated with different event types. In this case,

observed behaviors were classified as unknown. The NNGE algorithm uses the concept of singles to create rules for behaviors which cannot be generalized. We believe this will lead to the ability to classify cases which common path mining called unknown.

4.3 Non-nested Generalized Exemplars (NNGE) algorithm

NNGE is an instance based classifier in which the algorithm creates if then else like rules represented by generalized exemplars. Generalized exemplars may be singles in which case the exemplar represents exactly one example from the training database. Alternatively, generalized exemplars may be hyperrectangles which represent more than one example of the same class from the training database. After training, new examples are classified by calculating a modified a Euclidean distance metric from the example to all exemplars. The new example is classified as the class of the nearest exemplar. NNGE training and classification steps are discussed briefly in this section. NNGE can be used with nominal and continuous attributes. The attributes presented to NNGE for the case study in this work were nominalized using STEM.

4.3.1 Training the classifier

Training the NNGE algorithm is an incremental process which includes steps named classification, generalization, and dynamic feedback. Each labeled example in the training database is first classified by comparing the new example to all known hyperrectangles and single examples. The classification step in training uses the same methodology and distance metric as standalone NNGE classification (described below). Hyperrectangles are generalized rules which represent a class and single examples are previous examples of a class which do not fit into a hyperrectangle. The classification

step involves calculating the Euclidian distance from the new example to all hyperrectangles and single examples. Equation 4.1 is used as distance metric. The classification step returns the closest hyperrectangle or single example for the new example. If the new example's class matches the class of the hyperrectangle or single example returned from classification, then the returned hyperrectangle or single example are generalized to include the new example. Generalization of hyperrectangles involves growing the hyperrectangle to represent the new example. Generalization of a single example forms a new hyperrectangle which generalizes both the old single example and the new example. If the new example's class conflicts with the class of the hyperrectangle or single example returned by the classification step, the returned hyperrectangle must be adjusted by pruning out the conflicting example. Finally, during training dynamic feedback is used to adjust feature and exemplar weights used by the distance function.

The training data set contains a set of *m* examples, i.e. training instances $\{e^1, e^2, e^3, \dots, e^m\}$. Each example e^j is characterized by n attributes, $E_1,\dots,E_n$, and a class label. The objective of the algorithm is to create a set of generalized exemplars which is represented by a set of hyperrectangles $\{H^1, H^2, \dots, H^k\}$. Each hyperrectangle has *n* sides where each side is associated with an attribute index from training. A hyperrectangle side represents all observed states at that attribute index for that hyperrectangle. When a hyperrectangle is formed or grown each new attribute value for a given attribute index is combined with previously observed attributes using the disjunctive (or) combinatorial operator. The hyperrectangle is converted to an if/then statement using the conjunctive (and) and disjunctive (or) combinatorial operators. All

observed attributes for an attribute index are combined with the disjunctive operator. The terms from all attribute indices are combined with the conjunctive operator. Table 4.2 provides a simple example with 3 observed examples from the same class. The hyperrectangle for Class Q1 for the examples in Table 4.2 can be represented by the if/then/else expression in Figure 4.1.

Table 4.2 Example training database

Example	E_1	E_2	E_3	E_4	Class
e^1	S0	S2	S3		Q1
e^2	S0	S1	S2	S3	Q1
e^3	S0	S5	S2	S3	Q1

if ($E_1 \subset S0$) & ($E_2 \subset (S1 \mid S2 \mid S5)$) & ($E_3 \subset (S2 \mid S3)$) & ($E_4 \subset (S3)$)
then Class = Q1

Figure 4.1 Hyperrectangle in if/then/else form

NNGE ignores missing attributes and therefore missing attributes do not contribute to the calculated distance. This property is useful for cyber-power EIDS because different scenarios of interest have different lengths. NNGE is also sensitive to the order of attributes within an example. The order of system states for a given event is very important for a cyber-power EIDS because a sequence of the same states in a different order implies a different event.

4.3.2 Classification

During classification the observed example is compared to all hyperrectangles and singles using the distance metric shown in equation 4.1. The observed example is as a

member of the class of the nearest exemplar. In the event of tie, the class with the most exemplars at the minimum distance is chosen [68].

$$D(e^j, H^k) = W_H \sqrt{\sum_{i=1}^{n} \left(w_i \frac{d(E_i, H_i)}{E_i^{max} - E_i^{min}} \right)^2} \tag{4.1}$$

Equation 4.1 is used to calculate the distance between example e^j and a hyperrectangle H^k. Equation 4.2 defines the *d()* function for nominal attributes. Equation 4.3 defines the *d()* function for numerical attributes. The variable *i* in equations 4.1-4.3 is the attribute position. For equation 4.1, E_i^{max} and E_i^{min} define the observed range the i^{th} attribute. For nominal attributes the range is always 1. The weights w_i and W_H are adjusted during the training process to optimize classification fit.

$$d_{nom}(E_i, H_i) = \begin{Bmatrix} 0, & E_i \subset H_i \\ 1, & Otherwise \end{Bmatrix} \tag{4.2}$$

$$d_{num}(E_i, H_i) = \begin{cases} 0, & H_i^{min} \leq \mathrm{E} \leq H_i^{max} \\ H_i^{min} - E_i, & E_i < H_i^{min} \\ E_i - H_i^{max}, & E_i > H_i^{max} \end{cases} \tag{4.3}$$

4.4 Implementation of Non-Nested Generalized Exemplar (NNGE) algorithm for cyber-power events

An effective EIDS can be formed by preprocessing input data with the STEM algorithm and then using the NNGE algorithm for event classification. The following text describes how NNGE were combined and describes how the resulting EIDS was evaluated.

4.4.1 NNGE algorithm for cyber-power events

Cyber-power system events are unpredictable and random. As such training instances used with data mining algorithms may or may not represent a concept strongly. Instance based learning is useful when available training data weakly or does not represent the concept to be learned. Alternatively, rule induction methods are useful when the concepts to be learned are strongly represented. Combining instance based learning and rule induction methods for dynamic power system events is an optimal solution. NNGE combines instance based learning and rule induction. NNGE uses a hybrid version of a rule based classifier which combines a distance function and general exemplars which provide more comprehensive rules. With appropriate preprocessing of data, the classification performance of NNGE can be optimized. NNGE performs poorly if the input data is noisy [68]. Conflicting examples significantly reduce classification performance. Using the STEM algorithm described in Chapter 3 to preprocess cyber power system events minimizes the state space and number of rules generated by NNGE, and results in high classification accuracy, small classification time, and small model building time.

Figure 4.2 provides an overview of the NNGE+STEM based EIDS. Raw heterogeneous data was collected and preprocessed using the STEM algorithm. STEM produced an ordered list of states for each observed scenario. The lists of states were used as input to NNGE. The list of states represents all state changes associated with the event across its duration. Each list of states was labeled with the scenario class. Figure 4.2 shows data preprocessing, STEM, and classification process.

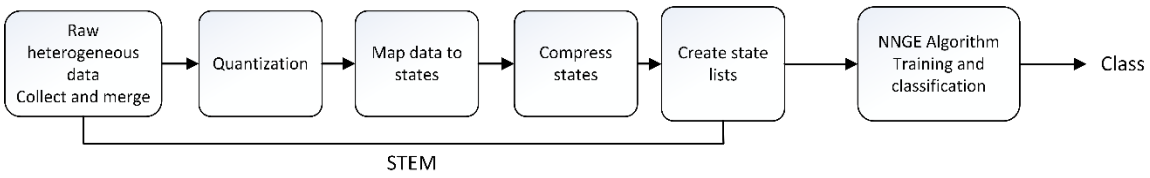


Figure 4.2 NNGE implementation for cyber-power events classification

An implementation of NNGE algorithm is available in the Waikato Environment for Knowledge Analysis (WEKA) software platform. WEKA is open source software which implements many state of the art machine learning algorithms [78]. WEKA uses the Attribute-Relation File Format (ARFF) for input data. All input data was processed to use this file format.

4.4.2 Evaluation method

NNGE was evaluated using k-fold cross validation. Cross validation is a commonly used method in a traditional batch setting to avoid over fitting issues. For each round of validation classification accuracy, kappa statistic, precision, true positive (TP) rate, and false positive (FP) rate were calculated. NNGE performance was compared to IDS performance metrics from [49] and [38].

Confusion matrices, also known as contingency or error matrices, are widely used to visualize the performance of a classification algorithm. Each column in the matrix is a predicted class whereas rows represents instances of an actual class. The confusion matrix provides information on classification accuracy, true positive (TP), true negative (TN), false negative (FN), and false positive (FP) that are used to evaluate the performance of an algorithm.

Classification accuracy is the ability of the model to correctly predict the class of the new examples. The classification accuracy is the number of correct classification predictions divided by the total number of instances.

$$Classificaition\ accuracy\ (\eta) = \frac{Correctly\ classified\ instances}{Total\ number\ of\ instances} = \frac{TP+TN}{TP+TN+FP+FN} \tag{4.4}$$

From the confusion matrix, the sum of diagonal elements represents the instances that are classified accurately and all entries not in the diagonal are incorrectly classified instances.

The true positive rate is the proportion of all instances that are classified as class 'x', among all the examples which truly are members of class 'x'. Recall is equivalent to true positive rate

$$True\ positive\ (TP)\ rate = \frac{TP}{TP+FN} = \frac{Diagonal\ element}{Sum\ over\ the\ relevant\ row} \tag{4.5}$$

The false positive rate is the proportion of instances that are classified as class 'x' but actually belong to a different class.

$$False\ positive\ (FP)\ rate = \frac{Column\ sum\ of\ class\ x - diagonal\ element}{Rows\ sums\ of\ all\ other\ classes} = \frac{FP}{FP+TN} \tag{4.6}$$

Precision is the proportion of instances that are truly members of class "x" among all the instances classified as class "x". Precision measures the positive predictive value. Precision is the measure of positive values which provides a sense of the false positive values when predicting a specific class.

F-measure is the combined measure of precision and recall. F-measure is the harmonic mean of precision and recall.

For true positive rate, precision, and F-measure, values approaching 1.0 indicate strong classification performance. Additionally, the classifier must have low false positive rates to provide better classification confidence.

In reality, power systems operate in normal conditions most of time. A data set sampled from a real power system would contain more than 99% normal operation data. The remaining part of the data would contain the events such as faults, outages, and attacks. If we evaluate the performance of an algorithm based on accuracy only, it may appear more effective than it actually is because of the large proportion of normal data.

Cohen et al. introduced the kappa statistic which is suitable for classification performance evaluation [79]. It is an analog correlation coefficient which provides statistical significance between the class label and attributes of instances. The accuracy is normalized by a chance predictor. The Kappa statistic is calculated using equation 4.7.

$$k = \frac{\rho_0 - \rho_c}{1 - \rho_c} \tag{4.7}$$

The variables ρ_0 and ρ_c are prequential accuracy and chance accuracy. If a classifier is always correct then k=1. Higher values of the kappa statistic signifies stronger statistical dependence.

The chance accuracy is calculated using the following equation 4.8 where N is the number of classes and m is the total number of instances.

$$\rho_c = \sum_{i=1}^{N} \left(\sum_{j=1}^{N} \left(\frac{C_{ij}}{m} \right) \sum_{j=1}^{N} \left(\frac{C_{ji}}{m} \right) \right) \tag{4.8}$$

The two datasets described in Chapter 2 were used to evaluate NNGE. The first dataset includes 10239 random cases of single line to ground (SLG) faults at random locations, SLG fault replay attacks, line maintenance scenarios, command injection cyber-attack scenarios, disabled relay during fault cyber-attack scenarios, and instances normal power system operation. The second dataset extends the first by adding double line (LL) fault scenarios, three phase to ground (3LG) fault scenarios, and repeated command injection cyber-attacks (aka. the Aurora attack [7]).

4.5 Results

Classification results using data mining algorithms depend on many factors including data processing, data labeling, and algorithm selection. Results are highly influenced by the selection of attributes. For the work presented in this chapter, the STEM algorithm was used to reduce data size. The reduced data size minimizes memory required to train and test instances while preserving key events and patterns in the dataset. STEM depends upon three parameters: the number and types of attributes used, attribute quantization interval, and the time window for state extraction. In this chapter, experiments 1, 2, and 3 were performed to select appropriate attributes, quantization intervals, and the time window. Experiment results were analyzed by comparing classification accuracy, kappa statistic, and the number of rules generated by varying the chosen attributes, quantization interval, and the time window.

Experiments 4 and 5 were performed to evaluate the NNGE algorithm based on the results from experiment 1, 2, and 3. In these experiments, NNGE was applied to multi-class and binary class datasets. Analysis of experiments 4 and 5 results support the

hypothesis that NNGE with STEM preprocessing provides effective classification for an EIDS.

4.5.1 Test data

The test data used for this work includes dataset 1 and dataset 2 as discussed in Chapter 2. The dataset 1 includes measurements and data logs associated with 10,237 simulated cases of 41 power system contingencies and cyber-attack scenarios. Detailed descriptions of the scenarios are provided in Appendix A. These scenarios consist of single line to ground SLG faults at variable locations in 1% increments from 10% to 90% on transmission line L1 and L2, SLG fault replay attacks on line L1 and L2, line L1 and L2 maintenance scenarios that mimic an operator remotely tripping relays to open a breaker at both ends of a transmission line, command injection attacks which illicitly trip a single relay, command injection attacks which illicitly trip two relays, attacks to disable primary protection of single relay in conjunction with a SLG fault, attacks to disable primary protection of single relay in conjunction with line maintenance, attacks to disable two relays in conjunction with a SLG fault, attacks to disable protection of 2 relays in conjunction with line maintenance, and finally normal power system operation. During all scenarios the load may be changed randomly from 200-400 MW.

Dataset 2 includes measurements and data logs associated with 11,715 simulated cases of 45 scenarios. Dataset scenarios include instances of all of the same scenarios present in dataset 1 and instances of 4 additional scenarios. The added scenarios include double line (LL) faults on line L1 and L2, double line to ground (2LG) faults on line L1 and L2, three phase to ground (3LG) faults, and Aurora attacks against relay R1.

The raw dataset is in comma separated values (CSV) format with labeled tuples that include 44 measurements and data logs (feature/attributes) in each row. The datasets were created by merging measurements from four PMUs, apparent impedance calculations, and log data from four relay event logs, four control panel logs, and four Snort logs. Phase voltages *(Va, Vb, Vc),* Phase current *(Ia, Ib, Ic)*, and frequency from each PMU were used. The synchrophasor data sample rate was 120 samples per second.

Execution of a single scenario consumes 2000-3000 tuples in the raw dataset which corresponds to approximately 16-25 seconds of simulation time. The STEM algorithm was applied to raw data. From STEM each measurement was quantized, then mapped to states, then state extraction was performed, and finally each case of a scenario was represented as sequence of states. Hence, the input to NNGE for this work was a list of states. WEKA was used to convert the sequence of states dataset to ARFF format and evaluate the NNGE algorithm.

4.5.2 Experiment 1: Attributes selection in STEM

In this experiment, the impact of attribute selection on the classification was studied. Table 4.3 shows the different attribute selection test cases considered for this experiment. STEM was used to process data for each case. Once lists of states were obtained from STEM, the output list of states were converted to ARFF format and the NNGE algorithm was used to classify the scenarios. For this analysis, multiclass classification was considered. There are 41 classes in the dataset 1. Six test cases, described in Table 4.3, were considered to compare the multiclass classification performance of NNGE algorithm with different selected attributes. Cases 1, 2, 3, and 4 evaluated NNGE plus STEM performance when just one of the 4 primary electrical

measurements was used (current, frequency, voltage, and impedance) in conjunction with the relay, control panel, and SNORT logs described above. Case 5 evaluated NNGE plus STEM performance when all electrical measurements are present, but, no logs are available. Finally, case 6 included evaluated NNGE plus STEM performance with all electrical measurements and all logs present.

Table 4.3 List of attributes for attribute selection test cases

Test case	Attributes
Case 1	Only three phase currents (Ia, Ib, Ic) from four relays/PMUs with all logs
Case 2	Only frequency from four relays/PMUs with all logs
Case 3	Only three phase voltage (Va, Vb, Vc) from four relays/PMUs with all logs
Case 4	Only apparent impedance seen by relay with all logs
Case 5	Three phase Voltage (Va, Vb, Vc), three phase current (Ia, Ib, Ic), impedance, frequency from four relays/PMUs without logs
Case 6	Three phase Voltage (Va, Vb, Vc), three phase current (Ia, Ib, Ic), impedance, frequency from four relays/PMUs , and all logs

One of the challenges for attribute selection when using STEM is that the states output from STEM depends upon the number and types of measurements input to STEM while the input to NNGE is the list of states. Commonly attribute selection methods implemented in WEKA are available to examine the value of states in the state list, but, cannot evaluate the attributes provided to STEM. To evaluate attribute selection multiple passes of STEM + NNGE for different groups of attributes were evaluated. Results were evaluated based upon resulting accuracy, the number of rules generated, and the number of states from STEM obtained using different attributes. Typically a smaller number of rules indicates a better model fit while a larger number of rules indicates a poor fit. Too

many inputs can lead to an increase in the number of states output from STEM without adding additional information. Too many states can be expressive of over fit. Alternatively, too few states may indicate a poor fit due to a lack of information related to events NNGE will classify. There is no heuristic to evaluate the number of rules or number of states directly. However, trends in the number of rules and number of states can be helpful in evaluated attribute selection.

Domain expert knowledge is one of the keys to successfully identify the appropriate attributes required to enable classification of particular event scenarios. A significant attribute for one event may not be significant for different type of event. Also, changes in measurements and data logs depend upon the type of event and the location of sensors. For example, during faults, current values for the faulted phase swing over a very large range, voltage dips significantly, frequency changes significant, impedance of the line changes significantly. For transmission line and generator loss, frequency excursion is significant but voltage and current values do not change as much when compared to faulted scenarios or changes slowly. Similarly, sensors close to the event location see more changes than the sensors farther from the event location. In general, a change in voltage and current will result in a change in impedance but limiting to an impedance calculation for all the scenarios may not reflect the true state of the system. The scenarios in the datasets used to evaluate NNGE cover a wide variety of event types and therefore have a wide variety of impacts on sensor measurements. As such, it is difficult to manually choose a particular attribute or a set of attributes for use with NNGE and STEM. Experiments were performed to individually analyze the classification

performances with different combinations of attributes to decide which attribute choices results in better classifier performance.

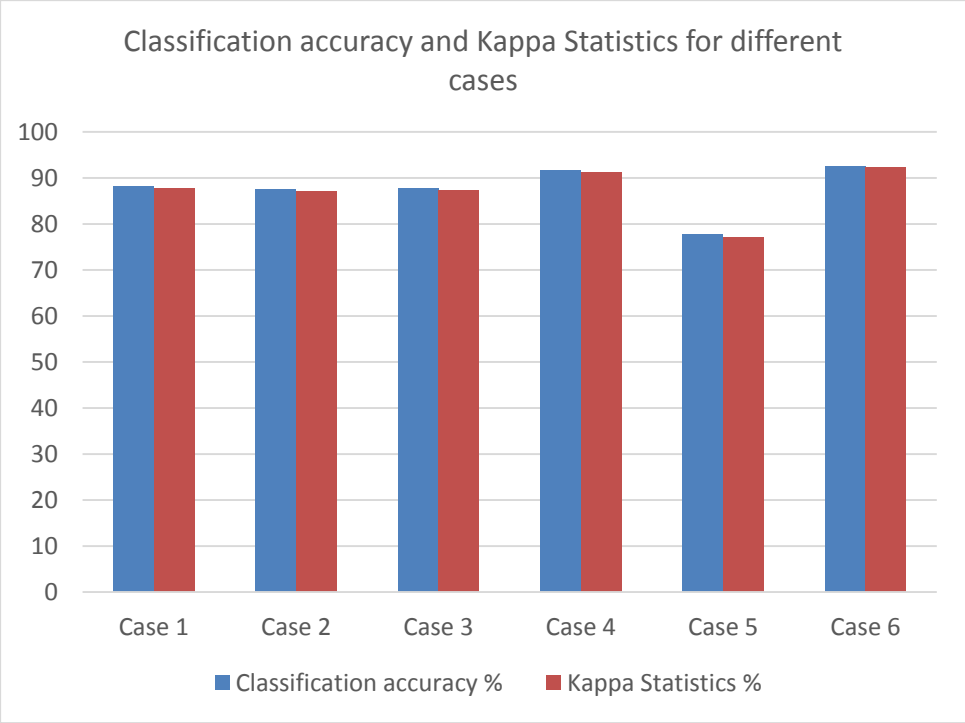


Figure 4.3 Classification accuracy and Kappa statistic for different attributes as input to NNGE

For cases 1-3, Classification accuracy and kappa statistic was approximately 87% when using only current, frequency, or voltage with logs and is shown in Figure 4.3. Analysis of confusion matrices (see appendix B) for these three cases revealed that major misclassification occurred among neighboring classes with similar scenarios. This suggest more information is needed to distinguish between the classes. Some of misclassification between non-similar scenarios was present among case 1, case 2, and case 3. For example, the frequency signature for attacks for faults when relays are

disabled by attack and SLG fault replays leads to the best classification when frequency data is present. Similarly, there were less number of matched states when using current attribute. Similarly, for classification of SLG faults versus and SLG fault replay attacks, availability of the current measurement led to less misclassifications than voltage and frequency. These examples suggest that classification of the broad spectrum of scenario types in the datasets is best achieved when all electrical measurements are available. For case 4, impedance with logs resulted better results than current, voltage, and frequency. Apparent impedance carries the information of both current and voltage. This suggest current and voltage together provide more useful information than separately and more information that frequency. Case 5 examined accuracy when all electrical measurements are present without logs. The case 5 accuracy was 78% and kappa statistic was 77%. Analysis of the confusion matrix (see appendix B) revealed that the majority misclassifications for case 5 were among the attack classes. The snort logs and control panel logs are critical information to distinguish line maintenance and command injection attack. The presence of a SNORT alert and control panel alert suggests valid line maintenance while the presence of only a SNORT alert without a control panel alert suggests an attack. Loss of this information resulted similar state sequences after STEM which caused more misclassification. Case 6 had the highest accuracy and kappa statistic at 93% and 92% respectively.

Figure 4.4 shows the number of rules generated for different cases. From the figure it can be observed that inclusion of more electrical measurement information helped reduce the number of rules. The number of rules was significantly higher with less attributes. One of the major influences on the number of rules was found to be the

number of unique states found in the dataset after STEM. The number of states for different cases is shown in Figure 4.5. In most cases, a higher number of states corresponded to a reduction in the number of rules generated by NNGE training. However, NNGE rules depend upon various factors including the number of unique states, dynamics of the system, and attribute selection

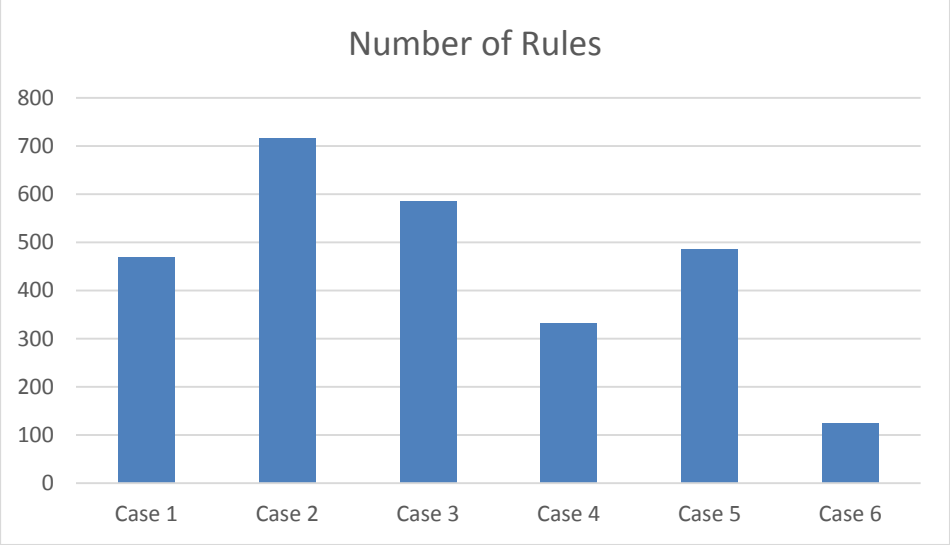


Figure 4.4 Number of rules generated by NNGE for different attributes

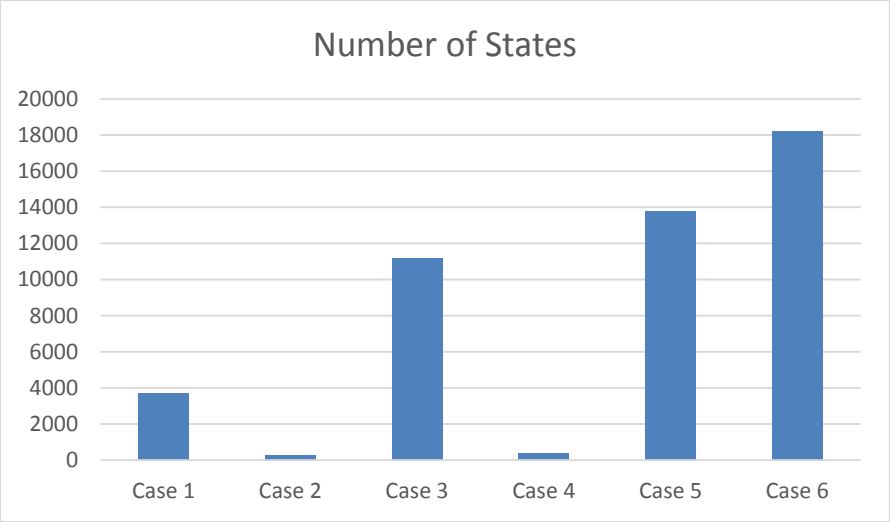


Figure 4.5 Number of states for different cases

Comparing these six attribute selection cases leads to multiple conclusions. First, the log information is critical for identifying cyber-attacks. Second, the combination of voltage, current, impedance, frequency, and logs (VIZF and logs) gives maximum accuracy and kappa statistic. Also, the combination of VIZF and logs led to a much smaller number of rules generated from NNGE training. Finally, measurement of the number of states did not provide useful information for attribute selection.

Based upon this analysis, VIZF and logs were chosen for use in subsequent experiments to evaluate NNGE + STEM. Although, the use of VIZF was optimal for this study, the details of classification revealed that there were improvements and degradation of classification performance for different cases. This suggests that the VIZF gives good performance when treating overall scenarios and measurements holistically. However, if a classifier was built to classify a limited set of scenarios a limited set of attributes may be optimal.

4.5.3 Experiment 2: Variable quantization interval in STEM

Experiment 2 was conducted to examine the impact of changing quantization intervals used by STEM on classification performance of NNGE. The STEM quantization interval should be adjusted for each selected numerical attribute. Each attribute will have a unique quantization interval. Quantization intervals may be selected using domain expertise or through quantitative study. For this work, quantization intervals for voltage, impedance, and frequency were selected using domain expertise. The quantization interval for current was chosen using a combination of domain expertise and quantitative study.

For voltage three quantization intervals were selected; low, normal, and high. The low, normal, and high intervals are [0-0.95] per unit (PU), [0.95-1.05] PU, and (1.05-∞] respectively. These ranges are suggested by national steady state voltage regulation standard for voltage monitoring applications. An examination of the scenarios in the datasets used to validate the NNGE+STEM EIDS showed that there are not scenarios which need voltage information outside of these ranges and therefore these ranges were adopted for this work. There are potential scenarios such as voltage oscillation and voltage dip that may require different voltage quantization intervals.

Frequency quantization is more complex. Choosing the quantization interval depends upon the interconnections and the type of control schemes. In the eastern interconnection under frequency load shedding starts at a threshold of 59.7 Hz. In ERCOT two frequency thresholds are used for load shedding. Load shedding 59.8 Hz and at 59.7 Hz a second group of loads are defined shed [65]. For this study, 59.8 Hz was

used as the threshold to define low frequency. No information was found on a high threshold. Therefore, high frequency was classified as above 60.2 Hz.

The impedance intervals were named for the distance protection zones; zone 1 (Z1), zone 2 (Z2), and normal (N). The Z1 interval was 0-80% of line impedance, Z2 is 80%-150%, and normal is greater than 150%.

Based upon domain expertise the initial quantization intervals for current were a range for low current, normal current, and high current. The low range was set to capture zero current and residual currents from measurement error and other factors. The low range was set to 0-110A. The normal range was set by considering standard practice for overcurrent protection schemes. Overcurrent protection schemes typically set the pickup current to twice the maximum load current. The maximum load current for all lines in the system was 500A. The intent of the high interval is to detect current in a fault state. Therefore the high range was set to start between the maximum load current and the pickup current. Through trial and error 700A was set as the top of the normal current range. The normal range was set to 110-700A. When relying solely on domain expertise current greater than 700A is high.

A quantitative study on current quantization intervals was conducted. In this study the normal and high intervals were divided into multiple smaller ranges to study the impact on classification accuracy, the number of NNGE rules created in training, and the number of unique states output from STEM. The quantization intervals used in this study are shown in table 4.4.

Table 4.4 Quantization intervals for different cases

Cases	Quantization intervals
Case 1	0 -110, 110-1200, 1200-∞
Case 2	0-110, 110- 700, 700-1200, 1200- ∞
Case 3	0-110, 110-500, 500-700, 700-900, 900-1200, 1200-1500, 1500-∞
Case 4	0-110, 110- 300, 300-500, 500-700, 700-900, 900-1200, 1200-1500, 1500-1800, 1800-∞
Case 5	0-110, 110-700, 700-900, 900-1200, 1200-1800, 1800-∞
Case 6	0-110, 110-700, 700-800, 800-900, 900-1000, 1000-1100, 1100-1200, 1200-1500, 1500-1800, 1800-∞

Figure 4.6 shows comparison of classification accuracy and kappa statistic among the six cases. Decreasing the quantization interval size, i.e. increasing the number of intervals, reduced both classification accuracy and the kappa statistic value. Case 1 and case 2 have relatively large quantization intervals. Case 3 and 4 were used to evaluate the effect of quantization intervals for normal currents. Case 5 and 6 were used to evaluate the impact of quantization intervals when current measures in the fault range. The study revealed that subdividing the normal current range into multiple intervals significantly degrades the classification accuracy. The poor accuracy for cases 3 and 4, subdividing the normal current range, was due to the fact that the quantization created more state transitions which did not provide information related to the classified scenario. The increased states sometimes provide multiple conflicting examples for the same scenario. Results for cases 5 and 6 showed that smaller interval ranges for the fault current range had little impact on classification accuracy. In contrast, the reason for higher classification accuracy for larger quantization intervals is due to the fact that the scenarios considered in this study have large changes in current, and as such larger quantization intervals are able to express the current change equally well.

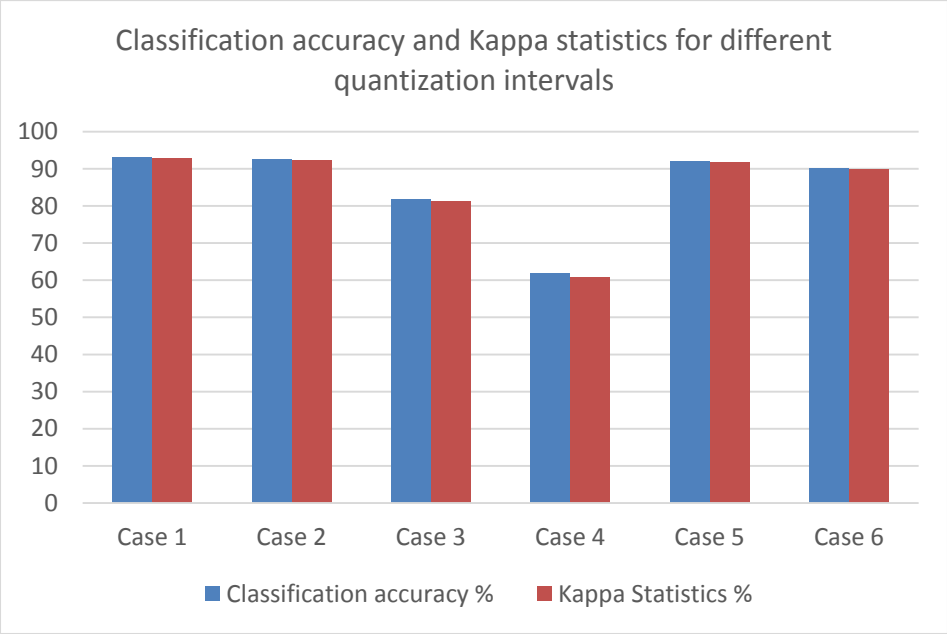


Figure 4.6 Comparison of classification accuracy and Kappa statistic for different quantization intervals

Figures 4.7 and 4.8 show the number of rules and number of states generated by NNGE + STEM algorithm respectively. It was observed that the relationship between rule generation and number of states is opposite. NNGE created more generalized rules with more states, more rules however results in lower accuracy and a lower kappa statistic value.

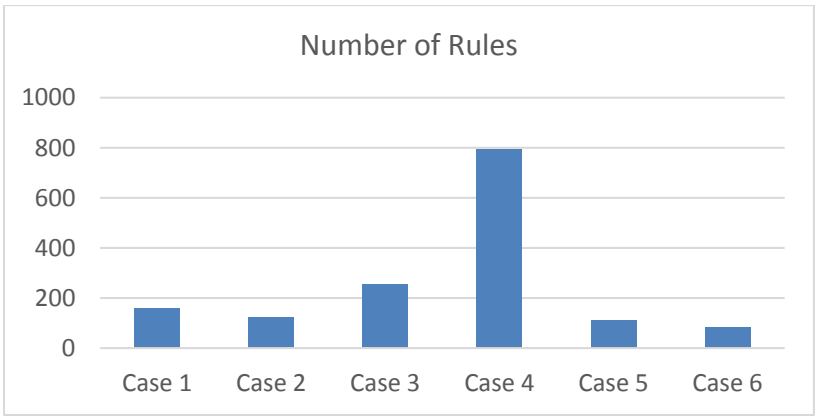


Figure 4.7 Number of rules generated by NNGE

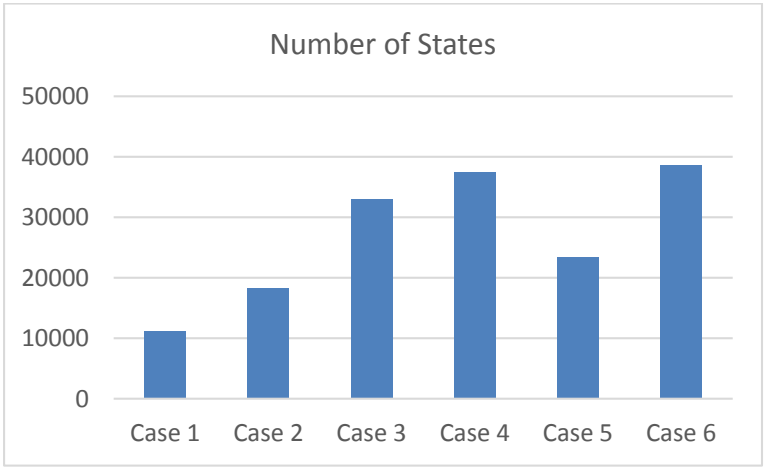


Figure 4.8 Number of states generated by STEM

From above analysis, the current quantization interval for case 2 was chosen as the appropriate current quantization interval for experiments 4 and 5. Case 1 and case 2 had similar classification accuracy. Case 2 had less rules generated in NNGE training. In general less rules implies faster classification and smaller memory usage, therefore, the quantization intervals from case 2 were selected for all future experiments.

The selection of quantization intervals for larger systems with many scenarios can be challenging. Careful study of each scenario to learn how sensor measurements change across scenarios is needed to choose effective quantization intervals. Each sensor's measurements should be carefully quantized so that the quantization interval captures the necessary patterns without introducing extra state changes which do not provide increased information related to the scenario.

4.5.4 Experiment 3: Variable time window in STEM

Experiment 3 was designed to evaluate the impact of STEM time window variation on NNGE classification performance. The STEM time window controls how many instances of a single state remain in a state list after compression when the system state is stable. This allows the input to NNGE to represent how long the system stays in a single state during a longer sequence of states. Increasing the STEM time window does not cause fast state changes to be removed from STEM output. All state changes are maintained in STEM output regardless of the STEM time window setting. The intent of this experiment is to test if NNGE classification accuracy is dependent on representation of the length of these periods of stability within state sequences. Decreasing the STEM time window increases fidelity to the original data but also increases the state space which may lead to a decrease NNGE classification accuracy.

For an example of the potential impact of STEM time window parameter, consider the two state lists from Table 4.5 for events 1 and 2 which are sequences of states related to events of class A and B respectively. The only difference between these events is the duration of the stable period the system stayed in state S1. If the STEM time window parameter is too high both events may be represented as (S0, S1, S2, S3)

after STEM, eliminating the distinguishing difference between them. If the STEM time window parameter is too low the length of all state lists may become too long and increase the state space of input data and lead to decrease classifier accuracy.

Table 4.5 An example of sequence of states

Event	State List	Class
1	S0, S1, S2, S3	A
2	S0, S1, S1, S1, S2, S3	B

All events from datasets 1 and 2 were used for this experiment. The attributes used in this experiment were three phase Voltage *(Va, Vb, Vc)*, three phase current *(Ia, Ib, Ic)*, impedance (Z), and frequency (F) from four relays (or PMUs) R1, R2, R3, and R4, and log information from relays, control panel, and SNORT.

The data rate after merging all STEM input variables was 120 samples per second which matches the Synchrophasor data rate. This data rate defines the maximum frequency of state changes and provides a lower limit for the STEM time window parameter of 8.33 milliseconds.

The fastest events in the datasets are faults and resulting relay operation. The distance protection zone 1 trip time was set for instantaneous relay operation for all experiments. The typical time for relay operation to a reflection of this event in a relay log or current measurement is on the order of 1-3 cycles (16.7 – 50ms). Another possibility a fast event pair of events is the time between 2 network packets. This time should be on the order of tens of milliseconds.

The slowest time between two events in the datasets should be the time between relay operation and automatic reclosing. This time is a relay setting and was set to 2 seconds for the experiments.

As such to test the effect of STEM time window parameter on NNGE classification accuracy the time window parameter was varied between 10ms and 2 seconds. The exact time window values used for comparison are shown in Table 4.6.

Table 4.6 Experiment cases

Case	Time window
Case 1	0.01 second time window
Case 2	0.1 second time window
Case 3	0.5 second time window
Case 4	1 second time window
Case 5	2 second time window

Figure 4.9 provides a comparison of classification accuracy and Kappa statistic for the different time window values used for this experiment. The time variation had very little effect on classification performance of the NNGE algorithm. The default time window of 0.5 second for all the above experiment was found to be optimal as compared to other time windows. The number of unique states created by STEM algorithms for all cases was same and was 18,193. This is expected since the number of unique states is not depended on the time window parameter. The constant number of unique states supports the assertion that increasing the STEM time window parameter setting does not because system state changes to be lost in STEM output. The number of rules generated by NGGE training was nearly the same for all STEM time window cases, as shown in Figure 4.10.

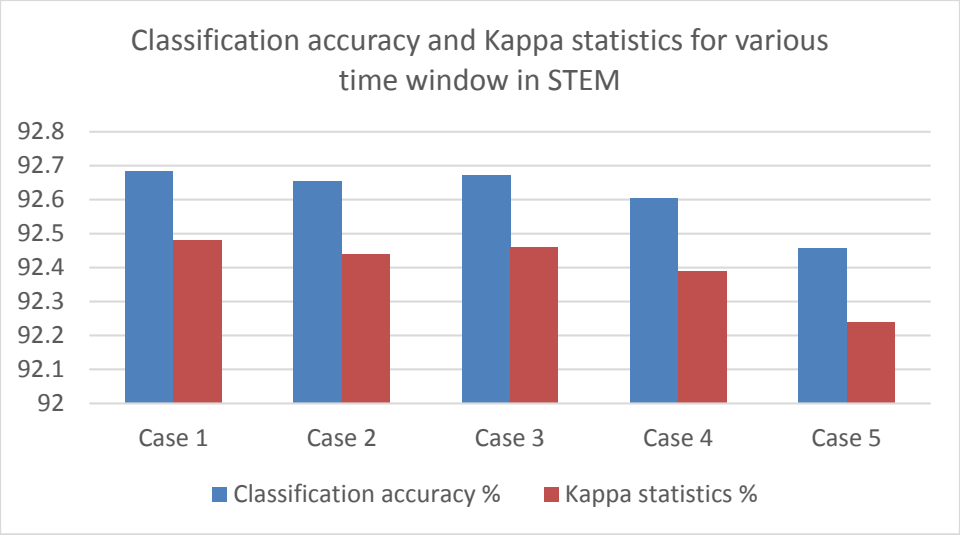


Figure 4.9 Comparison of classification accuracy and Kappa statistic

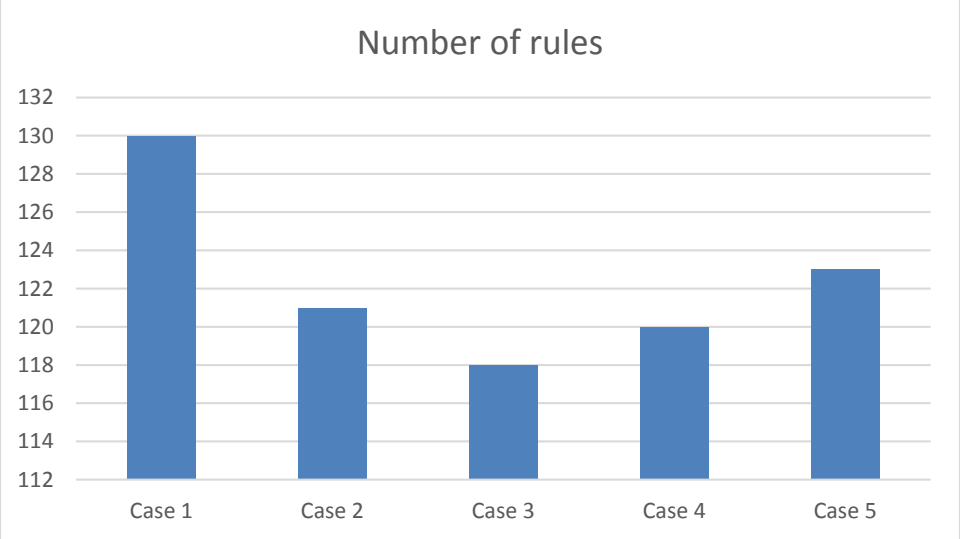


Figure 4.10 Number of rules generated by NNGE algorithms

The above results did not show significant variation in classification accuracy, Kappa statistic, or number of rules generated. The time window of 0.5 seconds had the best classification accuracy and Kappa statistic and the lowest number of rules generated

by NNGE training. As such, the STEM time window parameter values was set to 0.5 seconds for all remaining NNGE experiments. Based on these results, the same STEM time window parameter value was used for experiments related to Hoeffding Adaptive Tree (HAT) classification described in Chapter 5 of this dissertation.

4.5.5 Experiment 4: Performance of NNGE for multiclass classification

Experiment 4 was used to evaluate NNGE performance as an EIDS with multiclass classification. Datasets 1 and 2 were used for evaluation. All data was preprocessed using the STEM algorithm. The output from STEM, which was used as the input to NNGE training and classification was list of states for each event in datasets 1 and 2 respectively.

NNGE performance was evaluated using classification accuracy, kappa statistic, true positive rate, F-measure, and precision.

Dataset 1 included 41 scenarios are labeled from Q1-Q41 with a total of 10,237 instances of the 41 scenarios executed in random order with random system load. Dataset 2 included 45 scenarios labeled from Q1-Q45 with a total of 11,715 instances of the 45 scenarios executed in random order with random system load.

This experiment was conducted to evaluate NNGE algorithm's performance for cyber-power event classification. Quantized measurements are converted to state lists using STEM, the attributes change from measurements to state IDs. For this experiment, the attributes are states ID in each column and a row corresponds to a scenario case. The selection of attributes, quantization intervals, and time window was chosen according to the findings from experiments 1, 2, and 3.

Ten-fold cross validation was used for the evaluation. For dataset 1, NNGE training created 123 exemplars(s) including 107 hyperrectangles and 16 singles. The low number of rules supports low memory usage, and suggests a good model fit which improves classification accuracy. The NNGE model was built in 216.01 seconds. For dataset 2, NNGE created 136 exemplars, 113 hyperrectangles, and 23 singles. The NNGE model was built in 348.27 seconds. The NNGE created more rules for larger datasets and required more time to build the model.

Classification accuracy for dataset 1 was 92.6% with kappa statistic of 0.92 and 94.0% with kappa statistic of 0.94 for dataset 2. The algorithm performed very well on classification accuracy, kappa statistic, true positive rate, F-measure, and precision for both datasets. The true positive rate, F-measure, and precision are plotted in Figures 4.11 and 4.12 for datasets 1 and 2 respectively. All values are close to 1 which signifies strong algorithm performance. The FP rate was plotted for both datasets in Figure 4.13. Figures 4.14 and 4.15 are confusion matrices for datasets 1 and dataset 2 respectively. The confusion matrices are combined across all 10 rounds of validation.

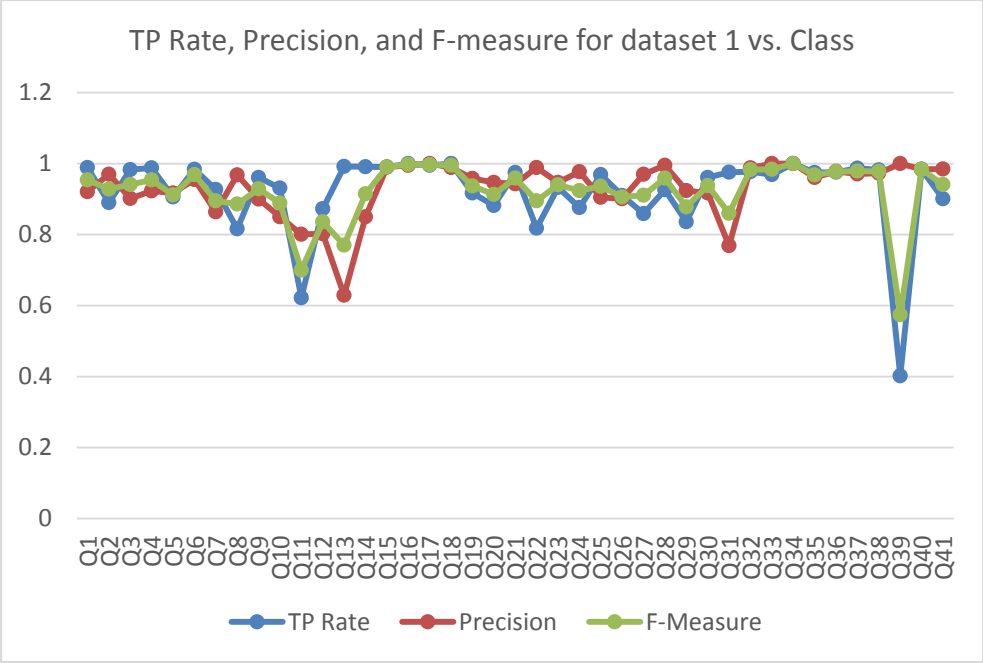


Figure 4.11 TP rate, precision, and F-measure for multiclass classification of dataset 1

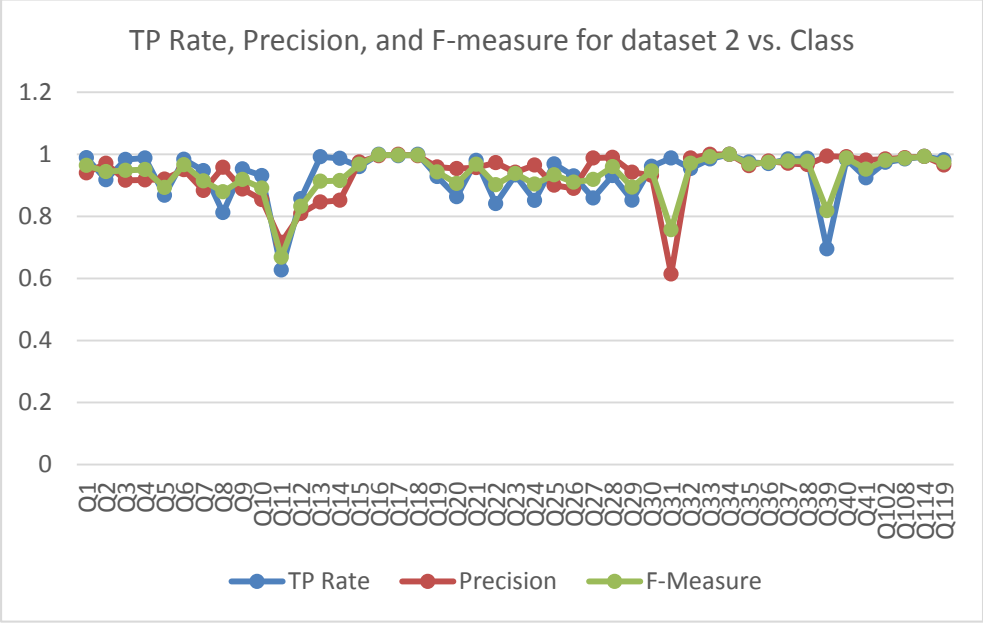


Figure 4.12 TP rate, precision, and F-measure for multiclass classification of dataset 2

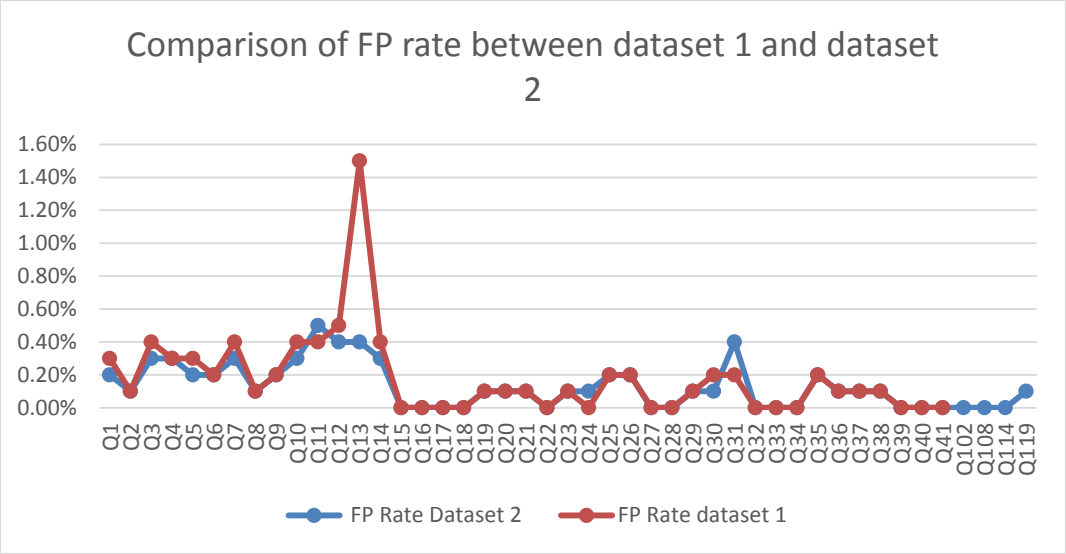
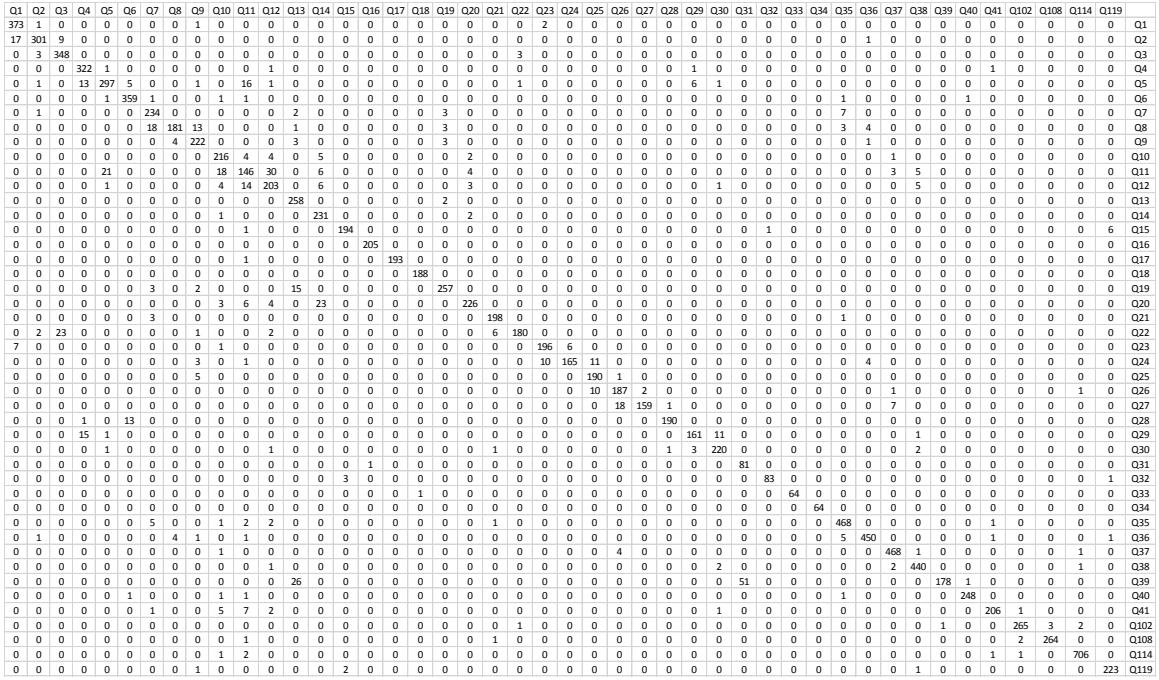


Figure 4.13 FP rate for scenarios in multiclass classification in dataset 1 and dataset 2

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
373	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
21	292	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q2
0	4	348	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	322	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	Q4
0	0	0	12	310	1	1	0	1	0	6	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	1	Q5
0	0	0	0	1	359	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2	0	Q6
0	1	0	0	0	0	229	1	0	0	0	0	2	0	0	0	0	0	3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	Q7
0	1	0	0	0	0	18	182	12	0	0	0	1	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	3	0	0	0	0	0	Q8
0	0	0	0	0	0	0	3	224	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q9
0	0	0	0	0	0	0	0	0	216	6	3	0	5	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	21	0	0	0	0	21	145	27	0	7	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	6	0	0	0	0	Q11
0	0	0	0	0	0	0	0	2	12	207	0	6	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	3	0	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	258	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	0	0	232	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	1	0	0	200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	3	0	3	0	0	0	17	0	0	0	0	0	254	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	3	5	1	0	22	0	0	0	0	0	231	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	197	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q21
0	1	25	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	10	175	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
10	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	196	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	9	170	9	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	Q24
1	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	190	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	11	183	4	0	0	0	0	0	0	0	0	1	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	17	159	1	0	0	0	0	0	0	0	7	0	0	0	1	Q27
0	0	0	0	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	189	0	0	0	0	0	0	0	1	0	0	0	0	Q28
0	0	0	15	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	158	14	0	0	0	0	0	1	0	0	0	0	Q29
0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	220	0	0	0	0	0	0	2	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	85	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	Q34
0	0	0	0	0	0	5	0	1	1	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	468	0	0	0	0	0	0	Q35
0	1	0	0	1	0	0	2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	453	1	0	0	0	0	Q36
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0	469	1	0	0	1	Q37
0	0	0	0	0	0	0	0	0	0	1	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	2	438	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	103	1	0	Q39
0	0	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	Q40
0	0	0	0	1	0	3	0	1	7	4	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	201	Q41

Figure 4.14 Confusion matrix for scenarios using state lists as input in dataset 1



Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	Q102	Q108	Q114	Q119	
373	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
17	301	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	Q2
0	3	348	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	322	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	Q4
0	1	0	13	297	5	0	0	1	0	16	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q5
0	0	0	0	1	359	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	Q6
0	1	0	0	0	0	234	0	0	0	0	0	2	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	Q7
0	0	0	0	0	18	181	13	0	0	0	1	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	4	0	0	0	0	0	0	0	0	0	0	Q8
0	0	0	0	0	0	0	4	222	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	Q9
0	0	0	0	0	0	0	0	0	216	4	4	0	5	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	21	0	0	0	0	18	146	30	0	6	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	Q11
0	0	0	1	0	0	0	0	4	14	203	0	6	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	258	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	1	0	0	0	231	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	1	0	0	194	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	6	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	3	0	2	0	0	0	15	0	0	0	0	0	257	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	3	6	4	0	23	0	0	0	0	0	226	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	198	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	Q21
0	2	23	0	0	0	0	0	1	0	0	2	0	0	0	0	0	0	0	0	0	6	180	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
7	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	196	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	0	3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	10	165	11	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	Q24
0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	190	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	187	2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18	159	1	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	Q27
0	0	0	1	0	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	190	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q28
0	0	0	15	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	161	11	0	0	0	0	0	0	1	0	0	0	0	0	0	0	Q29
0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	3	220	0	0	0	0	0	0	2	0	0	0	0	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	83	0	0	0	0	0	0	0	0	0	0	0	0	1	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	0	0	0	0	Q34
0	0	0	0	0	5	0	0	1	2	2	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	468	0	0	0	0	1	0	0	0	0	0	Q35
0	1	0	0	0	0	4	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	450	0	0	0	0	1	0	0	0	1	Q36
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	468	1	0	0	0	0	0	1	0	Q37
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	2	440	0	0	0	0	0	1	Q38
0	0	0	0	0	0	0	0	0	0	0	0	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	51	0	0	0	0	0	0	0	0	178	1	0	0	0	0	Q39
0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	248	0	0	0	0	Q40
0	0	0	0	0	1	0	0	5	7	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	206	1	0	0	Q41
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	265	3	2	Q102
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	264	0	0	Q108
0	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	706	0	Q114
0	0	0	0	0	0	0	0	1	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	223	Q119

Figure 4.15 Confusion matrix for scenarios using state lists as input in dataset 2

An analysis of classification accuracy was conducted. Scenarios with significant misclassification rates were examined. Examination of misclassifications noted in the confusion matrices provides explanation for peaks and valleys in the TP rate, Precision, F-Measure, and FP rate curves from Figures 4.11 – 4.13.

Scenarios (Q7-Q12) were often misclassified as each other. Each of these scenarios are instances of single line to ground faults replay attack. The only difference between the scenarios is the distance from the primary relay. The single line to faults were group by increasing distance. Pan et al. conducted a similar study with the same datasets [38]. Pan notes that misclassifications between similar single to ground faults categories occurs due to minor variations in relay operation time, breaker opening time, and measurement dynamics. These misclassifications are not critical as the main

objective of the EIDS is to distinguish valid fault events from cyber-attacks which may mimic such an event. Other technologies are available to power system operators to determine the fault distance.

Scenarios Q21-Q30 and Q35-38 are instances of cyber-attacks in which 1 (Q21-Q30) or 2 (Q31-Q38) relays have been disabled through a cyber-attack and then the transmission line is subjected to a fault. These scenarios are also group by the distance of the fault from the primary relay and also often are confused within these groups. Confusion with the groups of the same cyber-attack is acceptable.

Multiple instances of scenario Q19, a cyber-attack which send network packets to remotely operate relays, were misclassified as scenario Q13, a legitimate event in which an operator remotely operates relays to allow for line maintenance. This misclassification is bad. A cyber-attack is classified as a legitimate event. A sensor was placed at the operator's computer to log the operator's intent to remotely operate relays. A second sensor was placed at the relay to detect network packets with commands to operate the relay. The intent of this sensor arrangement was to provide a different signature for these two scenarios. Across both datasets scenario Q19 was correctly classified 92% of instances. So, the sensor arrangement provides good coverage, but, future work is needed to improve classifier accuracy between these scenarios. Scenarios Q20 and Q14 are similar to scenarios Q19 and Q13 respectively except the scenarios are performed on a different transmission line. Scenarios Q20 and Q14 had misclassification rates as Q19 and Q13 for the same reasons.

Multiple instances of scenario Q22, a cyber-attack in which relay R1 is disabled and a fault occurs on transmission line L1 was misclassified as scenario Q1, a single line

to ground fault on line L1. Because only relay R1 was disabled relay R2 operates. When relay 2 operates is removes the path to the load and the current drops to 0 amperes. The PMU measurements are similar for both scenarios because the both have similar outcomes. This causes the misclassifications.

The classification of scenario Q39, a cyber-attack disabled both relays on a transmission line when an operator remotely operates relays for line maintenance, was significantly low. The vast majority of misclassifications involve scenario Q39 misclassified as scenario Q13, a legitimate event in which an operator remotely operates relays to allow for line maintenance. Examination of the lists of states output from STEM for both scenarios revealed that in most cases the first 5 states for both scenarios are the same. NNGE classification ignores extra states when calculating the distance between an instance and a hyperrectangle or single example. Scenario Q39 is a simple event and only typically has 5 states. When NNGE calculates the distance between a new example of Q39, which is shorter than Q13, it ignores the extra states after the first 5 which match and calculates 0 distance between these scenarios. This is a bad result. Two scenarios which are obviously different because of their length are confused because the first N states match. To compensate for this issue another sensor may be added to force a difference between the scenarios with a common initial sequence of states. Adding a numeric value which is the length of the tuple as the first item in all tuples would cause the distance to be different between the two scenarios and likely fix this issue.

The average testing time per instance is plotted for all rounds of validation in Figure 4.16. The average testing time was slightly over 0.2 milliseconds. The 0.2 milliseconds test time is significantly faster than the current synchrophasor reporting time

(8.33 ms for 120 samples per second sample rate). Hence NNGE classification can be used in real time applications.

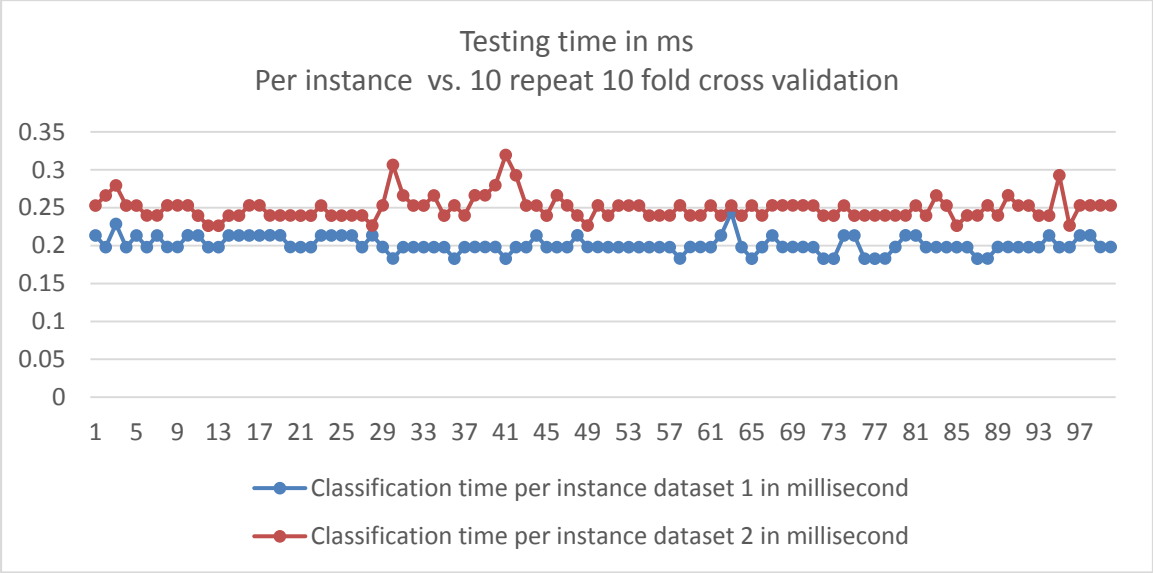


Figure 4.16 Testing time per instance in millisecond for dataset 1 and dataset 2

4.5.6 Experiment 5: Performance of NNGE for binary class classification

In this experiment, classification performance of NNGE algorithm for binary classification was evaluated. Both dataset 1 and 2 were used for this experiment. The STEM algorithm was used to obtain list of states for each scenarios. The scenarios were classified into two classes. All non-attacks scenarios were relabeled normal. All attack scenarios were relabeled as attack. Tables 4.7 and 4.8 shows how each scenario was relabeled for the 2 datasets.

Table 4.7 Binary Class Grouping for Dataset 1

Normal	Attack
Q1, Q2, Q3, Q4, Q5, Q6, Q13, Q14, Q41	Q7, Q8, Q9, Q10, Q11, Q12, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40

Table 4.8 Binary Class Grouping for Dataset 2

Normal	Attacks
Q1, Q2, Q3, Q4, Q5, Q6, Q13, Q14, Q41, Q102, Q108, Q114	Q7, Q8, Q9, Q10, Q11, Q12, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40, Q119

The algorithm performed well for binary class classification. The overall accuracy improved as compared to multiclass classification. The overall accuracy was 96% and 95% for datasets 1 and 2 respectively. The Kappa statistic was 0.9 for both datasets. NNGE less rules during training as compared to multiclass case. For dataset 1, training created 74 rules; 43 Hyperrectangles and 31 singles. The NNGE model was built in 43.49 seconds. For dataset 2, training created 79 rules; 51 Hyperrectangles and 28 singles. The NNGE model was built in 69.72 seconds. Dataset 2 had more rules due to the introduction of new scenarios. Also, the model built time increased due to larger dataset. The reduction in the number of rules when compared to multiclass classification signifies the algorithm was able to generalize rules more effectively for binary classification. In addition, the model built time was significantly reduced in binary cases than multiclass cases.

Table 4.9 Confusion Matrix for dataset 1

Attack	Normal	
7176	252	Attack
167	2642	Normal

Table 4.10 Confusion Matric for dataset 2

Attack	Normal	
7292	363	Attack
166	3894	Normal

Table 4.9 and 4.10 show confusion matrices for binary class classification. For dataset 1, approximately 3.4 % of attacks were classified as normal and approximately 6% of the normal events were classified as attacks. Analysis of the misclassifications between binary classes is difficult due to the large number of scenarios grouped together. However, from the multiclass analysis we know there were a significant number of cases of attacks classified as non-attacks and vice versa. The same reasons for misclassification are likely in the binary classification case.

Tables 4.11 and 4.12 show TP rate, FP rate, precision, and F-measure. TP rate, precision, and F-measure values signifies strong performance by NNGE.

Table 4.11 TP rate, FP rate, Precision, and F-measure for dataset 1

TP Rate	FP Rate	Precision	F-Measure	Class
0.97	0.06	0.98	0.97	Attack
0.94	0.03	0.91	0.93	Normal
0.96	0.05	0.96	0.96	Weighted Average

Table 4.12 TP rate, FP rate, Precision, and F-measure for dataset 2

TP Rate	FP Rate	Precision	F-Measure	Class
0.95	0.04	0.98	0.97	Attack
0.96	0.05	0.92	0.94	Normal
0.96	0.04	0.96	0.96	Weighted Average

Figure 4.17 shows the test time per instance in milliseconds. The average test time per instance was slightly higher than 0.2 millisecond. The testing time per instance is well below the current synchrophasor data rate which means binary classification can be performed in real time. The classification time is similar to the same metric for multiclass classification.

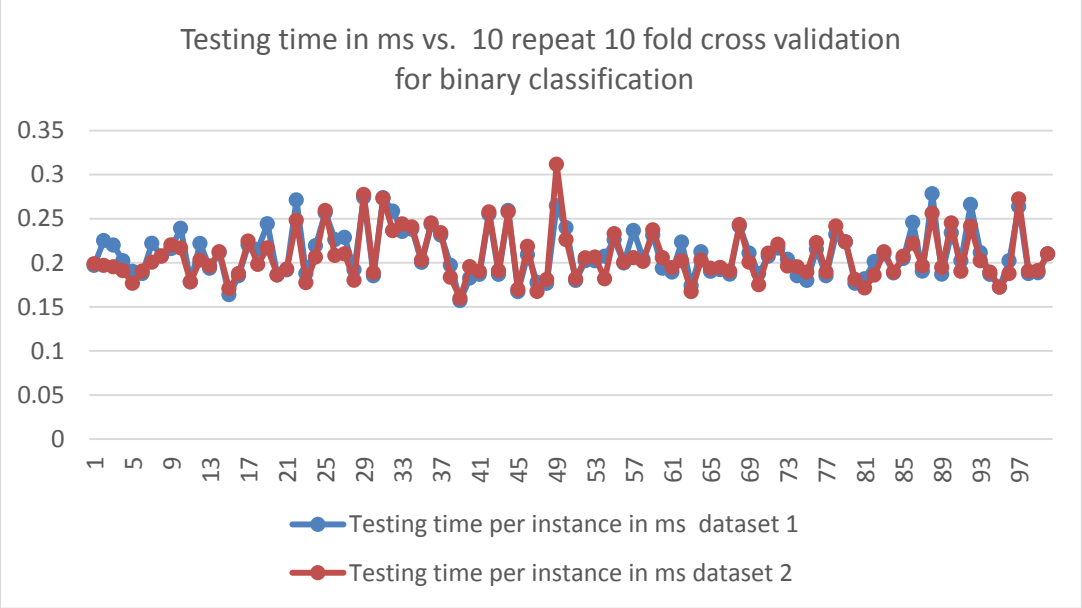


Figure 4.17 Testing time per instance in millisecond for dataset 1 and dataset 2

4.5.7 Comparison of performance of NNGE algorithms with other results in literature.

Event classification and intrusion detection for power systems is an emerging field of research. Datasets from the test bed described in this work have been used to evaluate other machine learning algorithms, common path mining [38] and other common machine learners [49], for suitability in classifying power system and cyber-attack events. Due to the evolution of the power system events, cyber-attacks, and datasets none of the works were evaluated with the exact same datasets. The Common path mining algorithm preprocessed data using the STEM algorithm, developed by the author of this dissertation, and then applied frequent item set mining. The work in [49] used selected a 1% random sample to preprocess the dataset before training and classification.

A comparison of all methods is presented in Table 4.13. Binary classification between the common path mining algorithm and NNGE has comparable accuracy. The NNGE multiclass evaluation included 45 scenarios while common path mining multiclass had 7 scenarios. STEM. NNGE had similar multiclass accuracy with more classes. The top performers from [49] were JRipper and Adaboost + JRip. The binary and three-class classification performed better than multiclass classification for JRipper, and Adaboost + JRip. Adaboost + JRip performed very well and is comparable to common path mining and NNGE + STEM. NNGE + STEM had the best performance for binary and broader multiclass classification as indicated by various performance indices in Table 4.13.

The evaluation presented in [49] included an evaluation of NNGE with a 1% random sample of raw data. STEM was not used to preprocess data with this algorithm.

The NNGE results without STEM are shown in Table 4.13 in the NNGE (No STEM) column. NNGE + STEM outperforms NNGE without STEM for all metrics.

Table 4.13 Comparison of NNGE with STEM to other algorithms

	JRip			Adaboost + JRip			Common Path Mining		NNGE (No STEM)		NNGE + STEM	
Number of classes	2	3	41	2	3	41	2	7	2	41	2	45
Accuracy	90%	90%	75%	95%	95%	90%	95%	93%	75%	25%	96%	94%
Precision	0.88	0.89	0.72	0.95	0.98	0.85	NA	0.98	0.52	0.33	0.969	0.943
Recall	0.70	0.85	0.60	0.91	0.93	0.80	NA	0.95	0.25	0.18	0.969	0.940
F-Measure	0.78	0.90	0.63	0.90	0.95	0.81	NA	0.96	0.18	0.18	0.969	0.939

4.6 Conclusion

This chapter presented an evaluation of the NNGE machine learning algorithm with STEM preprocessing for effectiveness as an event and intrusion detection system (EIDS) for cyber-power event classification. NNGE + STEM is suitable for classifying cyber-power events due to its ability to combine instance based learning and rule induction methods which provides excellent classification accuracy. Additionally, the ability of NNGE to generalize rules minimizes memory usage and provides fast classification. The ability of NNGE to handle sequential data makes it suitable for datasets in which each scenario is represented as a set of states in temporal order.

The experiments in this chapter demonstrated NNGE + STEM enables an excellent EIDS that can handle large WAMS heterogeneous data. The EIDS achieved more than 90% classification accuracy, greater than 90% kappa statistic, and classification times well below the current synchrophasor data reporting rate. These results demonstrate that an EIDS implemented using NNGE + STEM fulfills the EIDS requirements. Furthermore, the results demonstrate that traditional batch processing data

mining techniques can be applied if a proper data processing method is used to reduce the data size maintaining patterns in the datasets. NNGE + STEM performed very well as compared to existing results from literature.

Several experiments were performed to accommodate larger and diverse cyber and power scenarios. Similarly, performance of the NNGE algorithm with different attribute selection, STEM quantization intervals, and STEM time windows was evaluated. Significant changes in classification performance were observed with different attribute selection combinations. Combining Synchrophasor data with log information from various sources was found critical for cyber-attack classification. Varying the STEM quantization intervals for selected attributes has a significant impact on the classification performance. STEM quantization interval selection is highly dependent on the variable, the variable's role in state changes related to an event, and the events chosen for classification. The impact of varying the STEM time windows was found to be minimal.

CHAPTER V

APPLYING HOEFFDING ADAPTIVE TREE (HAT) FOR REAL TIME CYBER-POWER EVENT CLASSIFICATION

5.1 Introduction

High speed time synchronized WAMS data has the ability to provide near real time event information if information is extracted and analyzed properly. However, continuous streams of high speed data pose significant challenges in data storage, management, and handling. This research work evaluated a data stream mining technique based on Hoeffding trees to classify cyber-power system events to develop a real time EIDS. A real time EIDS must be able to process a stream of WAMS heterogeneous data, build a model on the fly, adapt to distribution changes in the data, use low memory, and have an evaluation time less than the synchrophasor data rate. Compressed quantized data and lists of system states obtained from the STEM algorithm were used as sequential input to evaluate the classification accuracy of the Hoeffding Adaptive Trees (HAT) algorithm augmented with the drift detection method (DDM) and adaptive windowing (ADWIN). Henceforth, the acronym HAT will be used to refer to HAT augmented with DDM and ADWIN. DDM is good to detect abrupt changes while ADWIN is used dynamically to detect abrupt and slow changes over time. Such change detection is suitable for power system WAMS data since WAMS data evolves over time and can undergo abrupt changes. This work provides three key contributions in the

development of a real time EIDS. First, unlike traditional batch processing methods, data stream mining using HAT provides a suitable way to handle an infinite series of data. Data storage and management issues are addressed by use of HAT. Second, the ability of the method to classify multiclass and binary class data in real or near real time provides a great opportunity to implement the method for a real system. Real time EIDS can be used to monitor and classify illicit and genuine cyber-power system events for real time situational awareness. Third, this work evaluates the suitability of the STEM algorithm for preprocessing data stream mining input. Two datasets "*dataset 1"* and "*dataset 2"* with 41 and 45 scenarios respectively were used to analyze HAT. The experiments performed in this work demonstrate that HAT was able to handle large WAMS heterogeneous data as a stream to build and update the model on the fly with a classification accuracy greater than 92% for multiclass and greater than 96% for binary classes. Also, the experiments demonstrate that HAT uses low memory and achieves low evaluation time faster than the synchrophasor data rate which enables development of an effective real time EIDS.

Data stream mining addresses the continuous data problem and can deal with very large data sizes. Data stream mining techniques can be applied to real time applications which are too large for classical machine learning and data mining techniques [6]. WAMS cyber power system event detection includes both large continuous streams of data and a need for real time classification. Data mining techniques have evolved to process large datasets, however, many algorithms still fail to address the problem of continuous data and evolving data streams. A classification algorithm for real time EIDS must meet some specific requirements to be suitable as an EIDS. The classification

method should be able to process a single example at a time, use limited memory, work in a limited amount of time, and be ready to predict at any time [19]. The requirements for real time EIDS in this work are summarized in Table 5.1.

Table 5.1 Real time EIDS requirements

Index	Requirements
1	The real time EIDS should be able to handle large WAMS data as an input stream.
2	The real time EIDS should be able to detect and adapt to concept changes in the data and update the classifier model.
3	The real time EIDS should be able to classify binary and a wide range of multiclass scenarios with high accuracy and kappa statistic.
4	The real time EIDS should use a low memory.
5	The real time EIDS should have fast evaluation time.

With continuous data, a single training process is not efficient since the previously created model cannot be updated when a new example arrives. The model may become outdated, and, hence, the single training method is inappropriate [19]. Data stream mining algorithms should be able to forget irrelevant past data and add new instances to create an updated model. Additionally, in the case of evolving data streams such as WAMS data, the algorithm must be able to detect changes and classify events.

HAT uses decision trees which are built by an incremental decision tree inducer that can deal with data streams with distribution and concept drift. HAT adapts and learns from the changing data streams over time and does not need a fixed sliding window in order to deal with the concept change or concept drift. HAT places frequency estimators at every node. ADWIN can be used as a change detector for HAT. One instance of ADWIN is used at each node to monitor the classification error rate. When a change is

detected, a new alternate subtree is created. The average error of the original subtree and the average error of the alternate subtree are compared and if there is a significant improvement with the alternate subtree, the original is replaced by the alternate [80]. HAT is a suitable candidate for WAMS data because it can process the data stream in real time, uses ADWIN and DDM for change detection, and includes a mechanism for forgetting old inferences and adding new inferences to continuously update the model. Also, the ability of HAT to handle nominal data and perform multiclass classification is useful as an EIDS [19].

The chapter is organized as follows. In section 5.2, a literature review is provided. The next section, 5.3, presents HAT for cyber-power events, algorithms, and evaluation methods. Section 5.4 and 5.5 present a power system case study with experiments and results.

5.2 Literature review

Many algorithms for dynamic data such as Hoeffding tree algorithms, very fast decision trees (VFDT), and concept-adapting very fast decision trees (CVFDT) [19] have been developed and applied. Data stream mining methods have been tested with various synthetic datasets and a very few real world datasets [39]. The authors in [39] highlighted the scarcity of real world datasets. The UCI ML [5] and KDD [48] are the most common sources of data that researchers use for machine learning algorithms. The UCI machine learning repository provides a few real world datasets. Forest cover type datasets, poker-hand datasets, and electricity datasets have been used to evaluate the performance of data stream mining algorithms [81]. The size of these datasets are very small, hence, these

datasets are not ideal for data stream mining [39]. Bifet et al. evaluated various data stream mining algorithms that can adaptively learn from data that changes over time [82]. A sliding window based Hoeffding window tree and Hoeffding adaptive tree were developed. The sliding window methods are based on the change detector and estimator and the implementation ensures theoretical guarantees. These algorithms were tested with synthetic data from the UCI repository. All of the above studies focused on improving the algorithm rather than exploring implementation to real world applications. This is mainly due to the lack of large datasets required to properly evaluate the method.

Data stream mining for power systems and cybersecurity are at the early stages of research. Dahal et al. evaluated data stream mining techniques for limited power system events with a limited number of instances [34] using only PMU data. Cyber-attacks were not considered in this study. Static and evolving data stream mining was explored using Hoeffding Trees (HT) and Hoeffding Adaptive Trees (HAT) respectively. The ability of the data stream mining technique to handle a wide variety of cyber-power scenarios, and larger datasets was not discussed.

Recently, a sliding window technique was implemented to classify events in real time. The TVA OpenPDC framework for real time modal and dampening analysis includes an oscillation monitoring system (OMS). Frequency domain analysis with Fast Fourier Transforms (FFT) was performed with a window of 7200 samples to detect oscillation. This method is promising for a particular event, however, the robustness of the method and its ability to classify multiple cyber-power events was not discussed [56]. Also, the analysis was performed only using synchrophasor data.

A method based on cloud computing environments which leverages parallel computing for storage, processing, and analyzing data collected from sensors to identify and predict machine faults is presented in [83]. Sequential sensor data such as trip and fail information from turbines is collected and a Case Based Reasoning (CBR) approach is implemented in Hadoop to achieve fault diagnostics locally and globally for online and offline cases. In the online model, the local computing node predicts faults but the local model relies on very limited cases of faults. The real time machine data is continuously monitored and the status is predicted. This method is used only for machine fault diagnostics and requires a pre-defined set of cases. Moreover, this method requires large quantities of compute resources as it leverages parallelization. In contrast, the HAT implementation in the Massive Online Framework (MOA) software does not require any special computing resources.

Gama et al. presented an electricity load forecast methodology which uses incremental clustering of data streams and incremental learning with a neural network [84]. The incremental clustering is based on a dissimilarity measure which depends upon correlation between time series. The neural network is incrementally trained with incoming data. This method has good performance on slow changing data. However, it does not perform well with abrupt or sudden changes in data which can occur in the case of WAMS data. Additionally, the incremental method requires more examples in order to reach neural network convergence.

Mustafa et al. presented an evaluation of various data stream mining algorithms available in the MOA framework [85]. The objective of this work was to find candidate data stream mining algorithms for the Advanced Metering Infrastructure (AMI). Seven

different algorithms were evaluated using a publicly available KDD cup dataset for AMI transactions. Also, simulated datasets with 5 different types of attacks were used in evaluation. The performance of the algorithms were presented in terms of accuracy, kappa statistic, running time, and model cost. The accuracy of classifiers was above 90%. This study is based on existing datasets and the scenarios include only limited cyber-attacks. The datasets contain only two classes of transactions, normal and attack, and the study did not consider any power system related scenarios. In the research presented in this chapter, the application of data stream mining for heterogeneous datasets is presented. Heterogeneous datasets require more data processing to achieve good classification results.

5.3 Hoeffding Adaptive Tree (HAT) for data stream mining

Among the different variants of HAT, in this work, HAT with ADWIN and DDM was studied for real time event classification.

Hoeffding Adaptive Tree (HAT) mining is based on Concept-adapting Very Fast Decision Trees (CVFDT). HAT is a modified version of the Hoeffding Tree (HT) algorithm [87]. The Hoeffding tree (HT) induction algorithm creates decision trees from the data stream and updates the tree after inspecting each example. The decision tree is constructed with an incremental design. Unlike traditional decision trees, HT does not require samples to be stored memory. The tree holds sufficient information in each node to grow the tree and perform classification [19]. Each node in the decision tree contains a test which depends upon the values of particular attributes. Hence, splitting a node is a crucial part of building a decision tree. The most popular node splitting method uses

information gain. The estimated information gain is a heuristic used to guide the splitting process. One of the key factors that influences decision making is an appropriate number of examples needed to achieve a minimum level of confidence. The Hoeffding bound is used to decide the minimum number of examples required to achieve a specified confidence [87].

Concepts are the target information that a model is trying to predict. Concept change is defined as change of the underlying concept over time. Concept drift represents a relatively slow change of the concept, whereas, concept shift represents an abrupt change in concept. HT cannot handle concept changes. So, HAT was developed to address concept changes in data. HAT is based on a sliding window in which the model is kept consistent within the sliding window of a data stream. The nodes store all relevant statistics. Every node in the tree has an estimator of frequency statistics. HAT with ADWIN uses one instance of ADWIN at each node to monitor the classification error rate. ADWIN is a parameter free adaptive size sliding window technique which can be used to detect change and trigger model revision [19]. ADWIN as used in the MOA setting uses a dynamically adjusted window. The size of the window increases when data is non-changing to increase accuracy and shrinks when it detects change. When a change is detected, a new alternate subtree is created without splitting the attribute. The average error of the original subtree and the average error of the alternate subtree is compared and if there is significant improvement with the alternate subtree, the original is replaced by the alternate subtree [80] [19]. ADWIN maintains a window that is statistically consistent in such a way that the average value inside the window does not change. If two sub-windows have a distinct average value, the older portion of the window is dropped [82].

DDM was included to address abrupt changes. DDM uses error rate to detect concept change and controls the number of errors produced by the model during prediction. For each point $'i'$ in a sequence, $'p_i'$ is the error rate of probability of misclassification with the standard deviation given by $S_i = \sqrt{\frac{p_i(1-p_i)}{i}}$. For a stationary data stream, the error rate of the learning algorithms will decrease when the number of instances increases. A significant change in the error rate indicates the change in class distribution and, hence, DDM triggers revision of the decision model. DDM compares the statistics of two windows: one with all data and another with the data from the beginning of the stream until the number of errors increases beyond a threshold. DDM works well with abrupt changes and does not perform well with very slow change [86].

5.4 Using HAT for real time cyber- power event detection

Power systems are monitored using various networked sensors which continuously measure system status and report measurements to the appropriate control center. Intelligent electronic devices (IED) such as PMUs have the ability to continuously monitor the power systems in real time with high speed synchronized measurements. Additionally, other IEDs, such as relays and meters, continuously send status to the control center to provide critical system information to operators and automatic controllers. A PMU sends a continuous stream of data which can practically be considered an infinite series of data. The velocity of PMU data can be very high, up to 120 samples per second. The volume of data continuously grows. Power system operation goes through both slow changes such as minor load variations and fast changes such as faults. Similarly, command injection attacks, response injection attacks, and other

cyber-attacks can create abrupt, incremental, gradual, or recurring changes. The changes are represented as concept drift and concept shifts in the datasets. One section of data plotting a time series of current measurements from a PMU is shown in Figure 5.1 to demonstrate slow and abrupt changes in data. The changes in the current data stream are related to faults, breaker opening, reclosing, and load changing events.

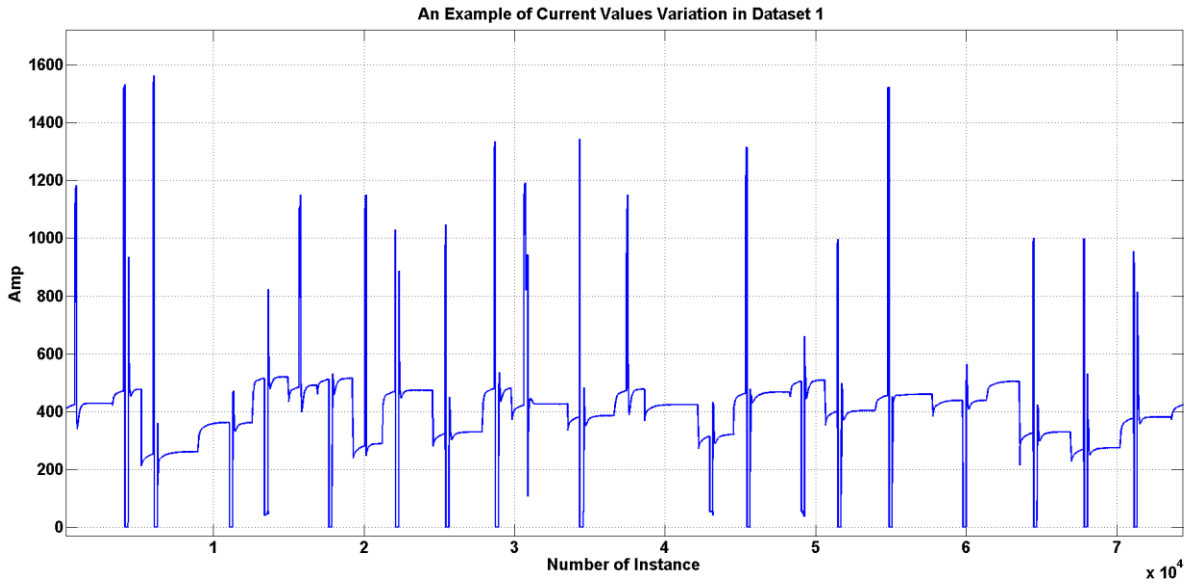


Figure 5.1 Current variation in dataset I

The heterogeneous datasets obtained from WAMS exhibit the properties of evolving data streams. The evolving data stream has three properties: an infinite series of data, high velocity, and concept and distribution of data changes over time, hence, past information becomes irrelevant and must be forgotten so the model can be updated to keep up with the data stream [19]. DDM with HAT as a base learner and with ADWIN is

suitable for classifying multiclass and binary class data with concept change in a data stream.

The Massive Online Analysis (MOA) is an open source framework for large scale data stream mining in real time. MOA includes collection of machine learning algorithms and tools to evaluate performance of algorithms. MOA also provides platform to implement new algorithms and provides an experimental framework for benchmarking data stream mining algorithms performance [19]. MOA framework implements HAT. Figure 5.2 shows the mining process used for this work. The STEM algorithm was used for data preprocessing. HAT can work with both numerical and nominal data. For this study, the nature of the datasets are heterogeneous, so, data preprocessing was used to convert all data to a nominal format. The input data to HAT was in the ARFF format. For this work, compressed state data from STEM was used as input to the HAT algorithm.

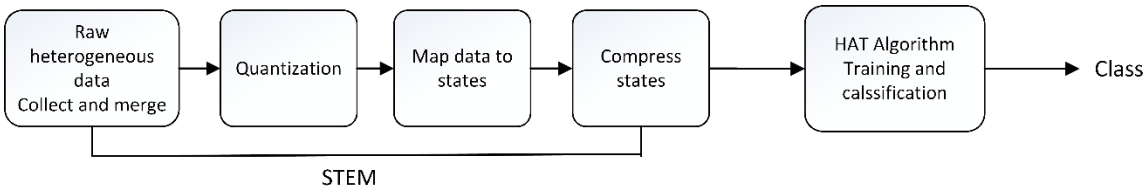


Figure 5.2 Implementation of HAT for real time cyber-power events classification

5.5 Results

The objective of the experiments presented in this section is to evaluate the ability of HAT to classify binary and multiclass datasets. The method was evaluated in terms of classification accuracy, Kappa statistic, RAM-Hours usage, and the time to classify each instance.

5.5.1 Evaluation metrics

There are multiple evaluation methods available in MOA. The ten-fold cross validation method is not suitable for the data stream setting because random parts of data streams cannot be separately reserved for training and testing. Hold out and prequential evaluation methods are commonly used in the stream mining setting. For this work, a prequential method was used. For prequential evaluation each individual sample is used to test the model and then used for training. Hold out is not necessary. The model is always being tested on the current example. This method makes maximum use of available data. With prequential evaluation, the statistics are updated with every example [19].

Classification accuracy, the kappa statistic, RAM-hours, and evaluation time were used to evaluate the performance of HAT. One RAM-hours is defined as every gigabyte of RAM deployed for one hour.

Cohen et al. introduced the kappa statistic which is suitable for stream classification performance evaluation. The accuracy is normalized by chance predictors. The kappa statistic is calculated using equation 5.1 [79].

$$k = \frac{\rho_0 - \rho_c}{1 - \rho_c} \tag{5.1}$$

The variables ρ_0 and ρ_c are prequential accuracy and chance accuracy. If a classifier is always correct then k=1. The chance accuracy is calculated using the following equation 5.2, where N is the number of classes and m is the total number of instances.

$$\rho_c = \sum_{i=1}^{N} \left(\sum_{j=1}^{N} \left(\frac{c_{ij}}{m} \right) \sum_{j=1}^{N} \left(\frac{c_{ji}}{m} \right) \right) \quad (5.2)$$

Power systems operate in normal conditions most of time. A real power system dataset would contain nearly all normal operation data. A small fraction of the data would contain information associated with events such as faults, outages, and cyber-attacks. If we evaluate the performance of an algorithm based only on accuracy, results may appear overly optimistic. The kappa statistic addresses this situation and provides a more realistic evaluation of the performance of the classifier.

5.5.2 Datasets for evaluation

Test data used for this work included dataset 1 and dataset 2 as discussed in Chapter 2 of this dissertation. Dataset 1 includes measurements and data logs associated with 10,237 simulated cases of the 41 scenarios from Q1-Q41. These scenarios consist of single line to ground (SLG) faults at variable locations in 1% increments from 10% to 90% on transmission line L1 and L2 (Q1-Q6), SLG fault replay attacks on line L1 and L2 (Q7-Q12), legitimately remotely operating relays to open breakers at both ends of a transmission line for line maintenance (Q13-Q14) , command injection attacks to illicitly operate single relay (Q15-Q18), command injection attacks to illicitly operate two relays (Q19-Q20), a single relay disabled during a SLG fault (Q21-Q30), a single relay disabled during line maintenance event (Q31-Q34), both relays protecting a line disabled and during SLG fault (Q35-Q38), both relays disabled during line maintenance event (Q39-Q40), and finally normal power system operation (Q41). The load is changed randomly from 200-400 MW.

The dataset 2 includes measurements and data logs associated with 11,715 simulated cases of 45 scenarios Q1-Q41 (described above), Q102, Q108, Q114, and Q119. The added scenarios include double line (LL) faults on lines L1 and L2 (Q102), double line to ground (2LG) faults on lines L1 and L2 (Q108), three phase to ground (3LG) faults on lines L1 and L2 (Q114), and repeated command injection attacks to rapidly open and close relay R1 called the 'Aurora attack' (Q119).

The raw dataset is in comma separated values (CSV) format with labeled tuples that include 44 electrical measurements and log data in each row. The datasets were created by merging measurements from four PMUs, four apparent impedance calculations, and log information that includes four relay event logs, four control panel logs, and four Snort logs. Electrical measurements included phase voltages *(Va, Vb, Vc),* phase current *(Ia, Ib, Ic)*, and frequency from each PMU. The synchrophasor data sample rate was 120 samples per second.

A case of a single scenario includes 2000-3000 tuples in the dataset that corresponds to approximately 20 seconds of simulation time. The STEM algorithm was applied to preprocess data. Each row of data was quantized, mapped to unique state IDs, then compression was performed to obtain the dataset used as input to HAT. Each row of the data was labeled with the corresponding scenario label. After STEM preprocessing, each scenario contains 30-40 rows (instances) of data. A row of input data contains 44 quantized attributes and a label. The compressed data contains concept change. WEKA was used to convert all data into ARFF format.

5.5.3 Experiment 1: Evaluation of performance of HAT using compressed dataset for binary classes

The objective of experiment 1 was to evaluate the HAT algorithm for binary classification of cyber-power events. D*ataset 1* and *Dataset 2* were relabeled with two classes of scenarios; *"normal"* for power system scenarios and *"attack"* for all cyber-attack scenarios. Table 5.2 shows which scenarios were added to each of the new classes. The total number of instances in dataset 1 and dataset 2 are 316,551 and 426,010 respectively. Both datasets contains random power system and cyber-attack scenarios and have significant concept change. Dataset 2 has added fault scenarios and has more abrupt changes.

Table 5.2 Scenario grouping for binary classification for dataset 1and dataset 2

Dataset 1		Dataset 2	
Normal	Attacks	Normal	Attacks
Q1, Q2, Q3, Q4, Q5, Q6, Q13, Q14, Q41	Q7, Q8, Q9, Q10, Q11, Q12, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40	Q1, Q2, Q3, Q4, Q5, Q6, Q13, Q14, Q41, Q102, Q108, Q114	Q7, Q8, Q9, Q10, Q11, Q12, Q15, Q16, Q17, Q18, Q19, Q20, Q21, Q22, Q23, Q24, Q25, Q26, Q27, Q28, Q29, Q30, Q31, Q32, Q33, Q34, Q35, Q36, Q37, Q38, Q39, Q40, Q119

HAT was used to classify compressed data. The comparison of classification accuracy and kappa statistic between dataset 1 and dataset 2 for binary classification are shown in Figure 5.3 and Figure 5.4. Algorithm performance was comparable for both datasets. The average classification accuracy and kappa statistic for both datasets were found to be above 95% and 90% respectively. The classification result was updated every

10,000 instances. Although, the accuracy shows some valleys, the algorithm recovered from the periods of low classification by continuously improving the model.

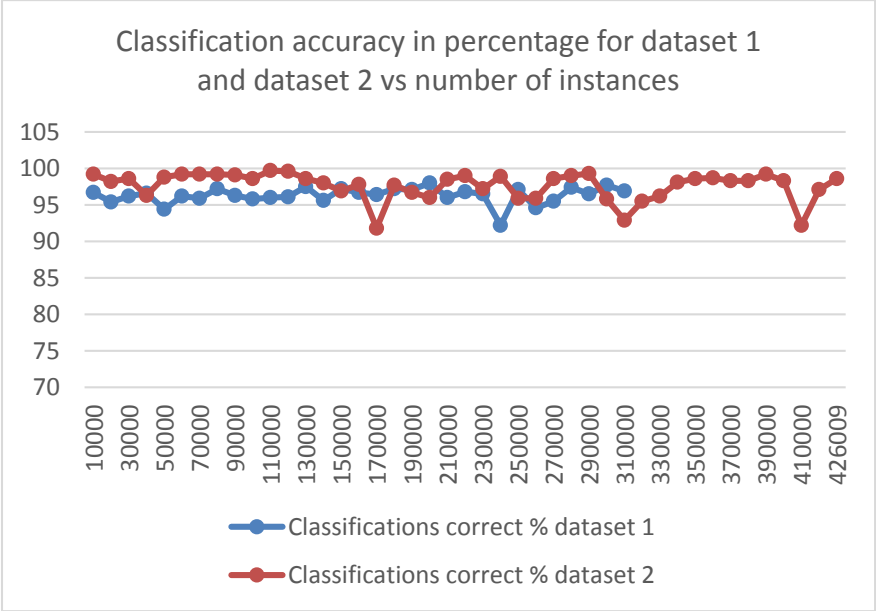


Figure 5.3 Classification accuracy (percent) vs. classified instance count for binary classification for dataset 1 and dataset 2

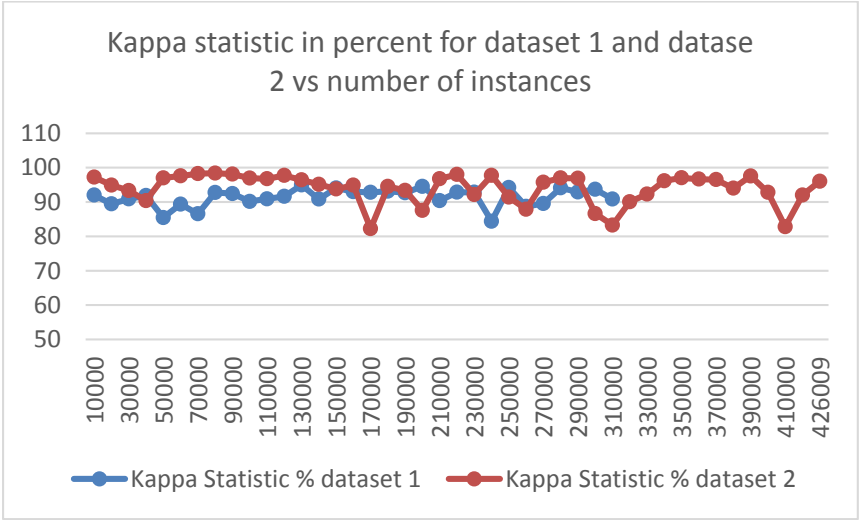


Figure 5.4 Kappa statistic (percent) vs. classified instance count for binary classification for dataset 1 and dataset 2

Figure 5.5 shows the number of changes detected by HAT as the datasets were processed. The change detection graph shows that the datasets contain significant concept changes. Even though the data contains significant changes, the classification accuracy remained high throughout the experiment, which signifies the ability of HAT to adapt to dynamically changing behavior of power system and attack scenarios. Dahal et al. pointed out non adaptive stream mining algorithms failed miserably in classifying such dynamic behaviors [34]. The HAT algorithm constantly updates its model whenever it detects changes and classifies events based on the updated model. The statistics to decide whether to update the old model depend on the Hoeffding bound that depends on the number of tuples (instances) available to build or update the model. The algorithm performed strongly as binary classification accuracy and the Kappa statistic were very high. The average classification accuracy for dataset 1 and dataset 2 was 96.39% and 97.68%, and the average Kappa statistic was 91.51% and 93.997% respectively.

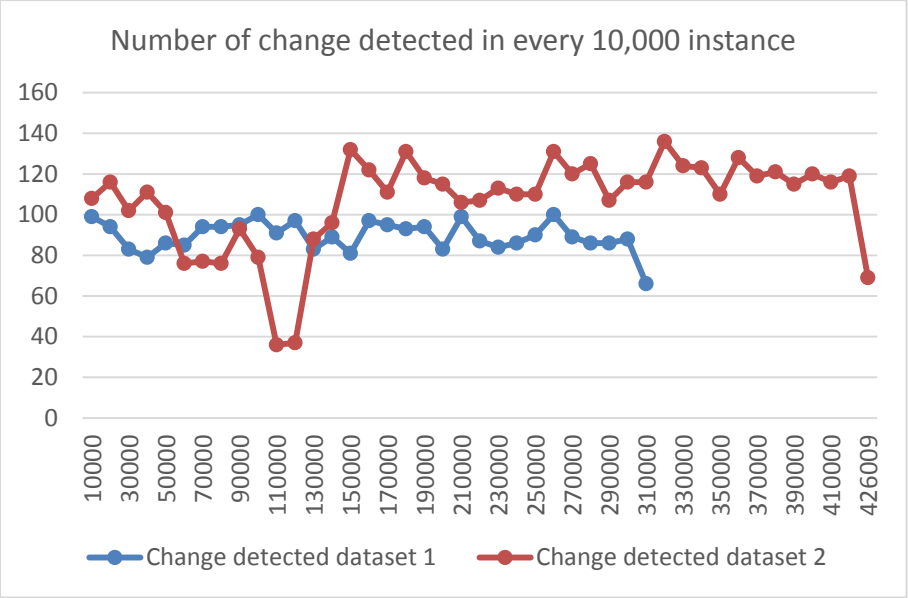


Figure 5.5 Number of change detected vs. classified instance count for binary classification for dataset 1 and dataset 2

The model cost can be expressed in RAM-Hours. RAM-Hours are the amount of RAM in gigabytes multiplied by duration of the experiment in hours. The RAM-Hours metric provides a sense of model size for a finite length of stream. Figure 5.6 presents the RAM-Hours metric as the datasets are streamed. The RAM-hours metric was similar for both datasets. The maximum RAM-Hours for dataset 1 and dataset 2 was 2.64×10^{-7} Gigabytes per hour and 2.26×10^{-7} Gigabytes per hour respectively. Figure 5.6 shows that the HAT uses very low memory to store the classifier model. The observed low memory use supports the notion that HAT memory use is low enough for use as an EIDS.

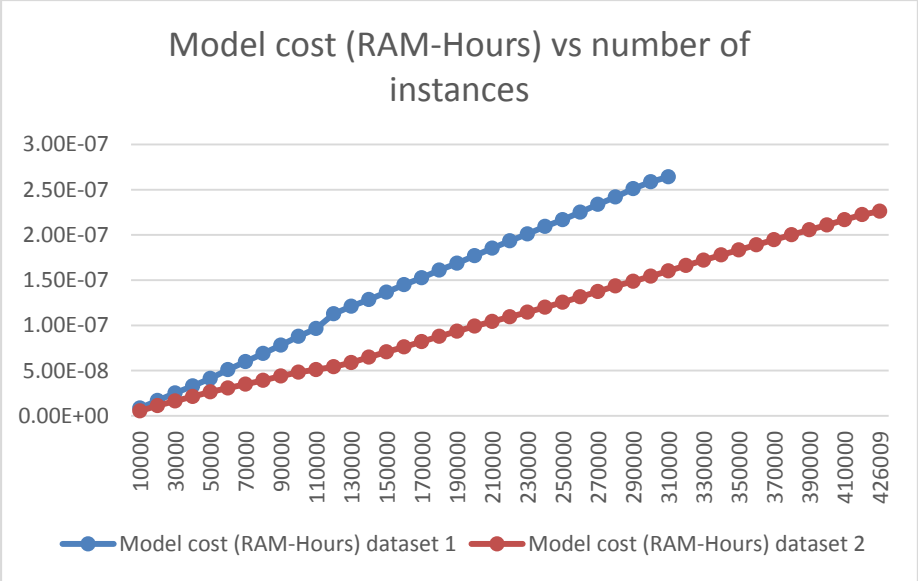


Figure 5.6 Model cost (RAM-Hours) vs. classified instance count for binary classification for dataset 1 and dataset 2

The average evaluation time per instance during the experiment was 36 microseconds (uS) for dataset 1 and 28 uS for dataset 2 as shown in Figure 5.7. Both cases had evaluation times per instance well below the current synchrophasor data rate of 8.33ms (corresponds to 120 samples per second). The low evaluation time per instance makes real time application of HAT as an EIDS possible.

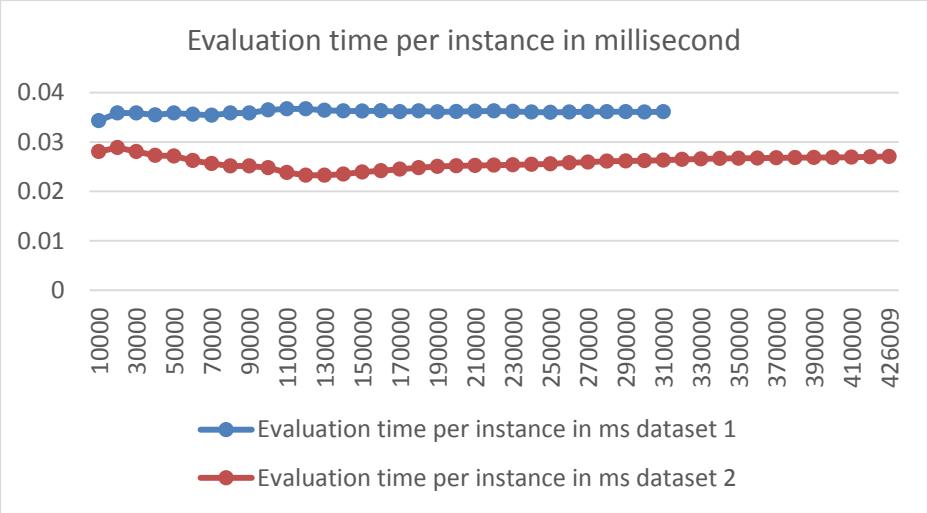


Figure 5.7 Evaluation time per instance in millisecond vs. classified instance count for binary classification for dataset 1 and dataset 2

5.5.4 Experiment 2: Evaluation of performance of HAT using compressed dataset for multi class

The objective of this experiment was to evaluate HAT algorithm for multiclass classification of cyber-power events. A comparison of performance of HAT using dataset 1 and dataset 2 is presented. Compressed data obtained from the STEM algorithm was provided as input to HAT for this experiment. Dataset 1 contains 41 scenarios labeled as Q1 to Q41.The dataset 2 contains 45 scenarios labeled as Q1 to Q45. The total number of instances in dataset 1 and dataset 2 are 316,551 and 426,010 respectively.

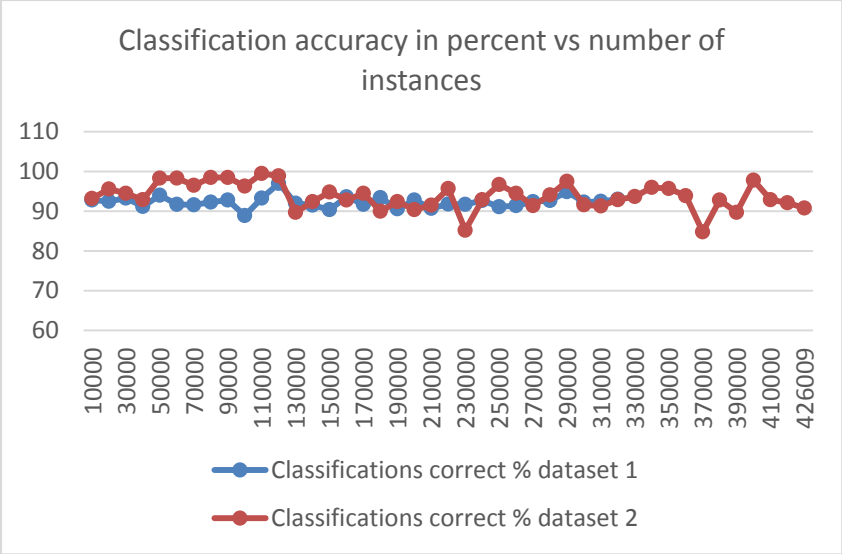


Figure 5.8 Classification accuracy vs. classified instance count for multiclass classification for dataset 1 and dataset 2

Classification accuracy for the multiclass classification problem is plotted in Figure 5.8. In the figure, classification accuracy and the kappa statistic were updated at every 10,000 instances. The average classification accuracy for dataset 1 and dataset 2 was 91.6% and 93.8% respectively. The accuracy decreased for multiclass case as compared to binary classification, but, is still high. The Kappa statistic for dataset 1 and dataset 2 averaged 90.9% and 93.1% respectively. High values of the Kappa statistic signifies that the HAT algorithm performed strongly for multiclass classification.

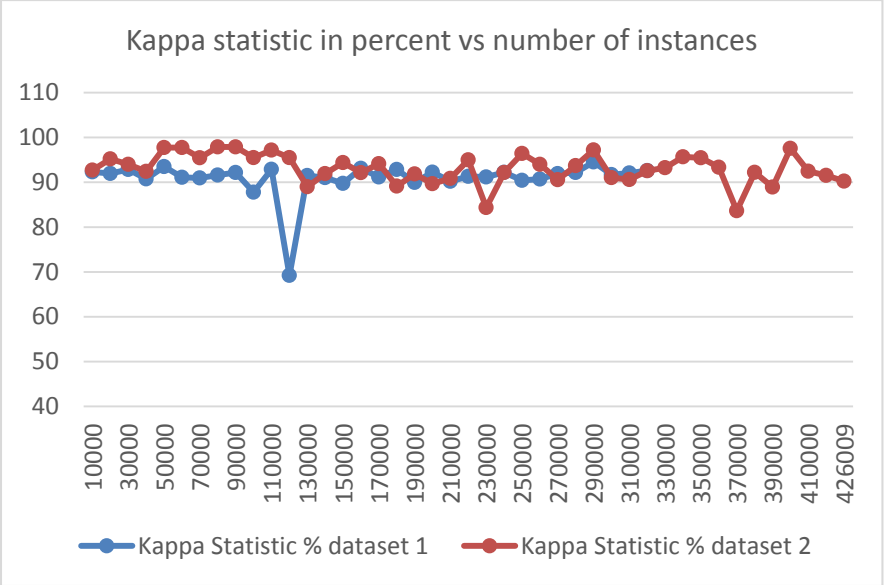


Figure 5.9 Kappa statistic vs. classified instance count for multiclass classification for dataset 1 and dataset 2

Figure 5.10 shows the number of changes detected in dataset 1 and dataset 2 every 10,000 tuples. HAT detected more changes in the multiclass case than binary class which reflects that the class distribution changes more often than in the binary case. This experiment demonstrated the ability of HAT to detect changes in the data, build the classifier model according to available instances, and adapt to the dynamic behavior of the power system yielding higher classification accuracy for a broad class of scenarios. Although, the classification accuracy contains some dips, classification accuracy always improved as the model retrained.

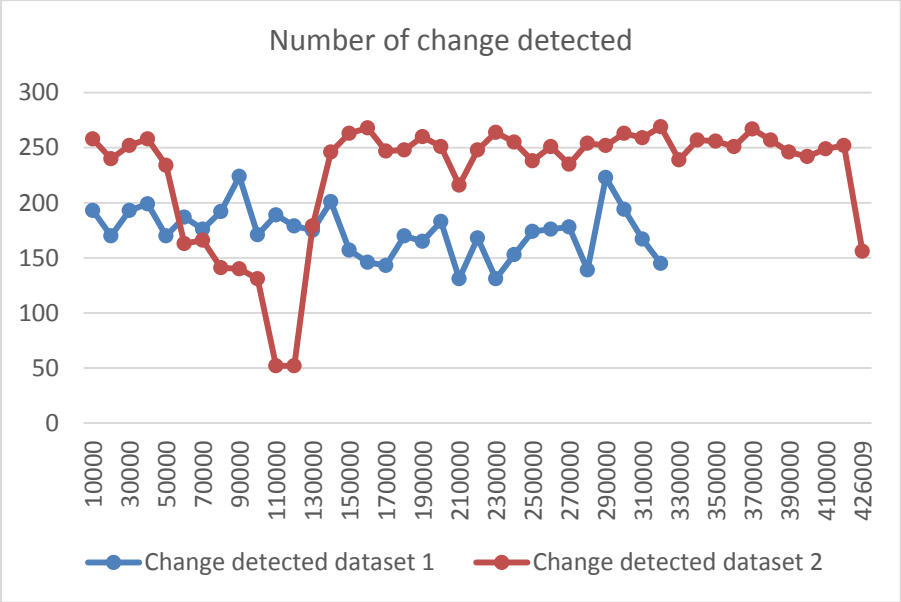


Figure 5.10 Number of changes detected vs. classified instance count for multiclass classification for dataset 1 and dataset 2

Figure 5.11 presents model cost in terms of the RAM-Hour metric for dataset 1 and dataset 2. The RAM-Hours metric value for dataset 1 and dataset 2 was 7.76×10^{-7} Gigabytes per hour and 7.16×10^{-7} Gigabytes per hour respectively. Binary classification required less RAM-Hours as compared to multiclass. This result also demonstrates that multiclass problems require more resources than binary class problems. The RAM-Hours metric for the multiclass case was still very low which is required for real time EIDS.

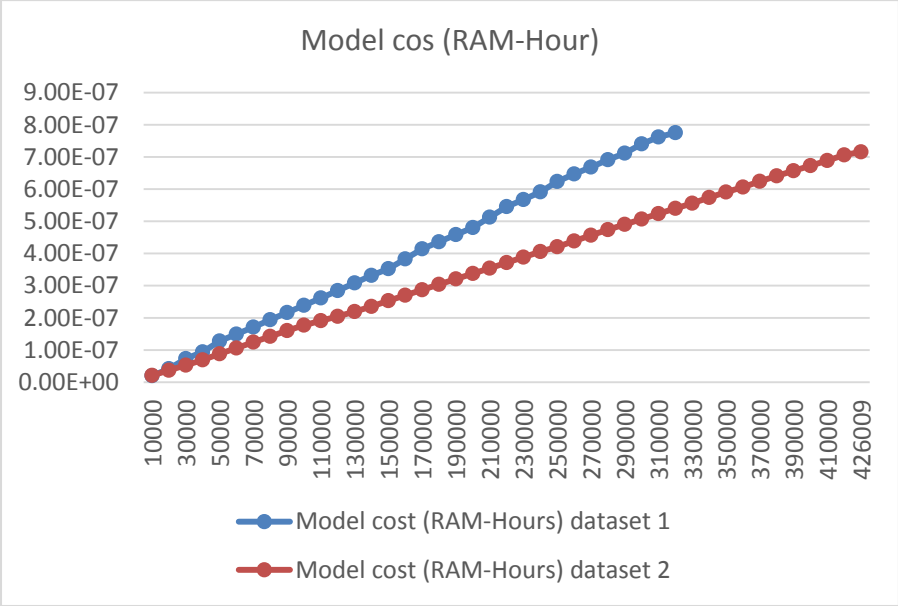


Figure 5.11 Model cost (RAM-Hours) vs. classified instance count for multiclass classification for dataset 1 and dataset 2

Figure 5.12 compares the evaluation time per instance in milliseconds for dataset 1 and dataset 2. The average evaluation time for dataset 1 and dataset 2 was 0.089 ms and 0.077 ms. Multiclass classification takes more classification time than the binary classification. However, the average evaluation time remains significantly below the current synchrophasor data rate which corresponds to 1 sample at every 8.33 ms.

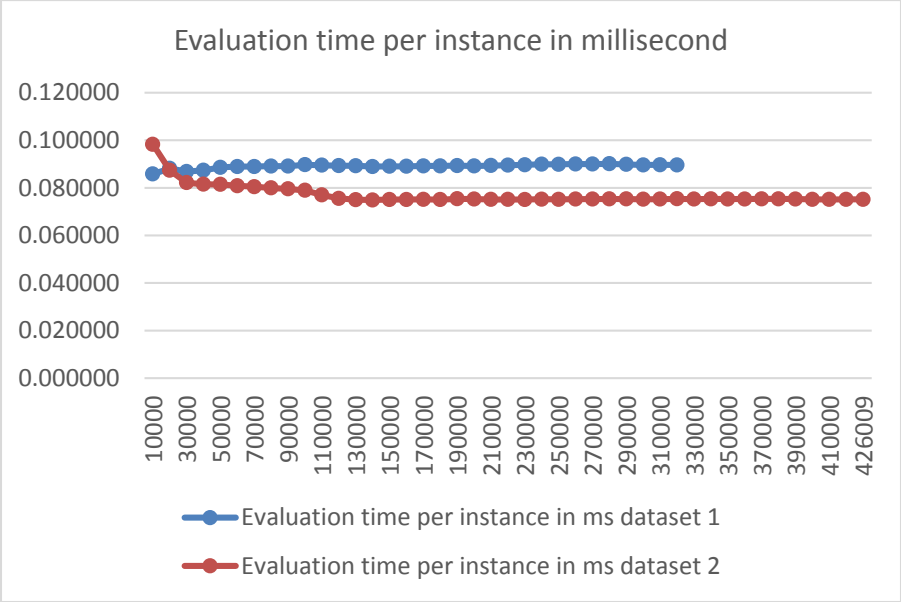


Figure 5.12 Evaluation time in millisecond per instances vs. classified instance count for multiclass classification for dataset 1 and dataset 2

5.5.5 Experiment 1 and 2 summary

Experiment 1 and experiment 2 demonstrate the ability of HAT to adapt to changes in streams of data. The datasets contain significant changes including fast changing events such as faults and slow changing events such as load changes. The classification accuracy and the kappa statistic show HAT adapted well after some temporary drops in classification accuracy. HAT performance demonstrates the usefulness of HAT for real time cyber-power event classification.

The binary and multiclass classification accuracy were comparable to the accuracy obtained from the traditional batch processing NNGE method presented in Chapter 4. This supports the hypothesis that data stream mining with HAT is applicable to classify the complex and broad scenarios associated with an EIDS and HAT can handle a large amount of data without sacrificing accuracy and computational resources.

HAT had better accuracy for binary classification. Binary classification is good for identifying legitimate and illegitimate events in a power system. However, binary classification insufficient to support automated responses for particular events. Even though, multiclass classification had lower accuracy than binary classification, multiclass classification should enable automated responses. Hence, multiclass classification is more desirable for detecting and classifying cyber-power events in power systems.

5.5.6 Comparison of HAT with other methods

The classification performance of HAT was compared with performance of other methods found in literature. HAT was compared with to Random Forest, JRip, Adaboost plus JRip, common path mining, and NNGE. Table 5.3 provides classification accuracy and the kappa statistic for each algorithm for binary and multiclass classification. The performance of HAT is very promising as the classification accuracy and Kappa statistic were among the best for all algorithms. The performance of HAT was comparable to Adaboost plus JRip, common path mining, and NNGE with STEM. HAT performed well for binary and multiclass classification. With low memory usage, small evaluation time, high accuracy, and the high Kappa statistic, HAT can be used to classify events and enhance situational awareness in the control room. HAT, as compared to other algorithms, can handle large datasets. Also, the ability of HAT to work with heterogeneous datasets with good performance makes it a favorable candidate for EIDS. As opposed to traditional batch processing methods, HAT can create a good model with less available data which is a significantly important property that is useful in the case of large stream datasets such as heterogeneous synchrophasor data [87].

Table 5.3 Comparison of HAT to other algorithms

	Random Forest [49]		JRip [49]		Adaboost + JRip [49]		Mining Common Path [38]		NNGE (No STEM) [49]		NNGE with STEM		HAT dataset 1		HAT dataset 2	
# of classes	2	41	2	41	2	41	2	7	2	41	2	45	2	41	2	45
Accuracy	75%	70%	90%	75%	95%	90%	95%	93%	75%	25%	95%	94%	96%	92%	98%	94%
Kappa	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	90%	94%	92%	91%	94%	93%

5.6 Conclusion and discussion

This chapter presents an evaluation of using HAT as a classifier in a real time EIDS. Experiment results show that HAT can be used to address concept drift and concept shift in datasets. The EIDS presented in this work achieved more than 96% accuracy for binary classification and more than 91% for multiclass classification. HAT also achieved very high Kappa statistics, very low RAM-hours, and very small evaluation times. A Kappa statistic value greater than 90% signifies that algorithm classification is reliable. HAT achieved excellent accuracy and stayed within memory and evaluation time computational boundaries. This shows HAT can be used for data stream mining to develop real time EIDS. HAT is suitable for large datasets and does not require large memory as opposed to traditional batch processing data mining techniques. The results showed HAT was able to classify a broad number of power system and cyber-attack scenarios and can be used in multiclass classification to generate automated response.

CHAPTER VI

DISCUSSION AND CONCLUSION

6.1 Conclusion

The ability of synchrophasor based Wide Area Measurement Systems (WAMS) to capture dynamics of power systems enables a paradigm shift in power system monitoring and control. WAMS open up many possibilities for real and non-real time applications using high speed time stamped data. The abundant data enables data mining algorithms related research and application development. However, data availability is a significant challenge faced by researchers, especially in universities and research institutes. Moreover, the big data produced by WAMS creates challenges in data handling, storage, and data transmission. The emergence of high speed data communication between Phasor Measurement Units (PMU), Phasor Data Concentrators (PDC), and control centers facilitates easy data transportation and provides better user control. However, the vulnerabilities in communication networks, protocols, devices, and software make WAMS prone to various types of cyber-attacks.

In this dissertation, a one of kind of WAMS cyber-physical power system test bed was developed by integrating a Real Time Digital Simulator (RTDS), physical relays, PMUs, PDCs, communication networks, and control and monitoring software. The test bed provides a platform to perform security testing and vulnerability assessment of various WAMS components and protocols [38] [54]. Moreover, the test bed addresses

the data unavailability problem for researchers by creating various datasets with a wide variety of scenarios. The unique ability of this test bed to create datasets related to power system events and cyber-physical attacks makes the test bed a valuable asset within the research community. Two datasets that contains thousands of random cases of power system faults, control actions, contingencies, and various cyber-attacks are available for researchers. The test bed and dataset products were used by researchers from Mississippi State University (MSU) and Oak Ridge National Lab (ORNL) to conduct multiple experiments. The test bed and dataset products have been used for power system cyber-attack impact studies [54], vulnerability assessments of WAMS devices and networks [43], data mining research using Synchrophasor data [50] [34], machine learning research for power system event detection [49], and intrusion detection system research [38]. Finally, the datasets created from the test bed were used in this dissertation to evaluate two EIDS using based on the NNGE and HAT data mining algorithms.

The datasets created by the test bed contain gigabytes of data. This volume of data presents a significant challenge when using data mining algorithms for cyber-power event detection and classification. The volume of data makes it difficult to apply traditional batch processing data mining techniques which require a significant portion available data be loaded into memory to build the classifier model. An effective data processing method was required to reduce the data size without losing key events and patterns in the data. A novel data processing and compression algorithm called STEM was developed. STEM merges asynchronous data from multiple sources and compresses data into list of system states. STEM is able to compress data size significantly while maintaining key events and patterns in the datasets. Since, STEM maintains labels at each

step of the algorithm, output from any step can be used for data mining input. The output from STEM depends upon the number of attributes, attribute quantization intervals, and a time window used for state extraction. Various experiments were performed to analyze the impact of these parameters in Chapter 4. The use of STEM algorithm in support of common path mining [38], NNGE, and HAT proves STEM's importance in data mining.

Ageing and networked infrastructure are vulnerable to many failures and cyber-attacks. The advancement of computational abilities within power system infrastructure also introduces potential cyber vulnerabilities which can be illicitly exploited by attackers. Concise and contextual information on detected events and intrusions delivered in timely manner can enable appropriate responses which protect the power grid and make it resilient to cyber-attacks and other contingencies. This dissertation presents a NNGE data mining algorithm to be used with STEM to create an effective Event and Intrusion detection Systems (EIDS). NNGE uses a hybrid modelling approach that combines the concept of a distance function and rule based learning. NNGE uses generalized exemplars as rules to classify events. The generalization reduces classification time without sacrificing accuracy [68]. The use of STEM with NNGE enables better generalization as STEM represents each event with a set of states lists which itself is a rule. Hence, the combination of STEM and NNGE creates faster, more reliable and accurate EIDS.

For NNGE with STEM, several experiments were performed to analyze the impact of attribute selection, attribute quantization intervals, and the time window used with STEM. Second, different experiments were carried out to demonstrate the classification performance of NNGE with STEM for the proposed EIDS. The

experiments on attribute selection enable the important conclusion that all events may not be effectively classified with same set of attributes. The impact of attributes on classification was variable for different types of events. Domain expert knowledge is required to effectively select appropriate attributes that impact classification of a particular event. Similarly, the selection of quantization interval also depends upon the types events and requires domain expert knowledge to optimally select intervals for each attribute. The STEM time window had very little effect on classification. In this dissertation work, a holistic approach was used to decide the appropriate number of attributes, quantization intervals, and time window. NNGE has excellent classification accuracy for the power system EIDS problem. The multiclass and binary classification accuracy of 93% and 96% respectively are the best classification accuracy as compared to other algorithms from literature. Other performance indices for NNGE with STEM showed that the algorithm is reliable and has very fast testing time which makes NNGE a suitable algorithm to create EIDS. These experiments demonstrate the ability of NNGE to create rules that can be used to classify binary classes formed from a very wide variety of power system and cyber-attack events. The consistency in performance for all type of scenarios indicates that NNGE can be used to classify a wide variety of cyber-power scenarios.

An alternative to the traditional batch processing data mining algorithm was also explored in this dissertation to address the data storage and the application of EIDS in real time. The application of Hoeffding Adaptive Tree (HAT) with DDM and ADWIN for cyber-power events classification in power system was studied. HAT is a family of decision tree based classifiers which are incremental learners. The ability of HAT to

adapt to constantly changing data makes HAT a suitable classifier to deal with the dynamic behavior of cyber-physical power systems. Also, the ability of HAT to work with data streams makes HAT suitable for real time applications including real time EIDS. In this work, output from STEM was used as input data to HAT. Experiments for binary and multiclass classification demonstrated HAT adapts to concept change in the data very well by updating the classifier model with new data without degrading the classification performance. The classification accuracy of 96% and 98% for binary class and 92% and 94% for multiclass for two datasets demonstrates consistency in performance. Also, the low memory and time required for HAT demonstrates the ability of HAT to produce a robust classifier model without exhausting memory while maintaining very high classification accuracy. This ability enables HAT to be used for very large volumes of data with a high speed data stream.

In this research work, NNGE, a traditional batch processing method and HAT, a stream mining algorithm were evaluated in terms of their ability to classify cyber-power events and their suitability for cyber-power event detection. Even though the research objective for both cases was the same, these methods provided various advantages individually.

NNGE demonstrated the ability to classify a broad range of scenarios with high accuracy but significant data processing was required to achieve success. NNGE requires all data to be present in memory to build the model and does not build and update the model in real time. The inability of NNGE to build and update model in real time naturally makes NNGE an offline analysis tool. However, since NNGE experiments demonstrated the time required to classify an instance is in the order of milliseconds (less

the synchrophasor data rate), NNGE can be used in real time applications. First, an instance of an NNGE model can be built offline with available data, then the incoming data can be converted into states using windowing. These states can be fed into the NNGE model to classify sequence of states. Although, the model does not change and cannot adapt with evolving scenarios, periodic retraining may solve the issue. Expert knowledge can be used to determine the periodicity of retraining the NNGE model. The offline classification is useful for post event analysis.

HAT on the other hand is suitable for the data stream setting where scenarios are constantly evolving. HAT is suitable for real time applications as it builds models with limited number of incoming data points. HAT addresses memory issues by using an incremental learning technique and does not store instances. As data evolves HAT adapts to changes by updating its model. Hence offline retraining is not necessary with HAT. The classification accuracy, Kappa statistic, and classification time using HAT was comparable to performance of traditional batch processing methods. One of the biggest challenges of HAT is all supervised learning requires labeling of instances which is not available in a real stream setting. Researchers are working on addressing this issue by using active learning [89].

Table 6.1 summarizes the work performed in this dissertation.

Table 6.1 Summary of the dissertation

Index	Contribution	Description
1	Developed a WAMS cyber-physical power system test bed	This one of kind test bed provides a platform for security testing, vulnerability assessment, and datasets for various researchers.
2	Developed datasets for power system event detection, intrusion detection and classification research	Datasets created using this test bed were used in power system event detection, machine learning, and EIDS research. Datasets have been used for published works from MSU and external researchers.
3	Developed STEM data processing and compression algorithm	This novel algorithm to compress WAMS heterogeneous data with compression ratios up to 4178 to 1. Compression is achieved without losing key events and patterns in the data.
4	Developed an EIDS using NNGE with STEM	The NNGE algorithm with STEM is suitable to develop an effective EIDS. The high classification accuracy, above 92% for multiclass and above 95% for binary class, high Kappa statistic, high true positive rate, low false positive rate less than 5%, and very low classification time less than current synchrophasor data rate fulfill all the EIDS requirements. The use of STEM with NNGE demonstrates that a NNGE with STEM EIDS can handle big data. The training and classification processes can be automated which lowers EIDS cost as compared to methods where rules are created manually [88].
5	Developed a real time EIDS using HAT augmented with DDM and ADWIN	HAT with DDM and ADWIN can be used to classify events with constantly changing behavior of power grid to create an effective real time EIDS. Experiment results include high accuracy, above 92% for multiclass and above 95% for multiclass, low memory usage, small time for classification, and ability to handle the big datasets in stream form.

6.2 Discussion and future works

This dissertation enables multiple possible future works. The test bed is able to simulate a wide variety of scenarios but still does not include many scenarios such a bus faults, switching shunts, and coordinated and more complex attacks. As such, the test bed work can be extended to include such scenarios.

The dissertation demonstrated a novel data processing and compression algorithm STEM for large heterogeneous data where the output of STEM depends upon attribute selection, attribute quantization intervals, and a time window parameter. Traditional methods of attribute selection in data mining do not work with STEM since it transforms measurements into state IDs. Several experiments were performed to find optimal combinations of attributes. However, a strong conclusion was difficult to make. This dissertation developed an EIDS that works for a 3 bus 2-line system with two zone distance protection and made use of 44 measurements. For example, the search for an optimal combination of two attributes results in 946 possible outcomes and finding an optimal combination using experimental methods is impossible. A heuristic is needed to aid attribute selection when using STEM. Similarly, a larger quantization interval performed better than a large number of smaller intervals. Domain expert knowledge was found valuable in selecting quantization intervals for chosen attributes. Additional work is needed to develop a heuristic for evaluating attribute quantization intervals.

The dissertation used a holistic approach to select the attributes, quantization intervals, and time window, however, the experiments demonstrated different attributes and quantization intervals revealed classification of some scenarios improved with particular attributes and quantization intervals, while classification of some scenarios

degraded. Rather than using the same attributes and quantization intervals for all scenarios, it is better to identify optimal attributes and quantization intervals for a particular scenario or set of scenarios. One possible option for the future work to address this issue is to divide an EIDS into multiple instances of EIDS, as shows in Figure 6.1, that have optimal attributes and intervals for particular scenario or group of scenarios. Using this approach, EIDS accuracy can be increased and more a reliable EIDS can be developed.

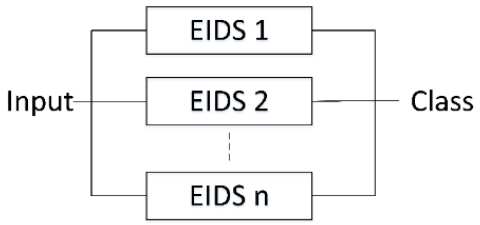


Figure 6.1 Instances of EIDS for optimal parameter selection and better accuracy

Additionally, the dissertation made use of only PMU measurements and data logs. However, in reality, for large power systems PMU data may not be available for each substation. In this case, the inclusion of outputs from state estimation be necessary. Future research should be directed to accommodate the output from state estimators and other sensors which help to scale the EIDS reach.

This dissertation also presented two EIDS based on NNGE and HAT for cyber-physical power systems. However, the EIDS considered only three substations and data from four PMUs. In reality, thousands of substations exist. Future work should address the scalability of EIDS implementation. The methods used in this dissertation can be

scaled to as many protection zones that a relay monitors. The STEM algorithm is scalable linearly as it only requires the addition of measurements. But a single EIDS for a large number of substations may not be effective due to large memory requirements and more processing time which makes EIDS training and classification slower. An ideal case of EIDS implementation would be monitoring each substation with one EIDS. However, cost may become an issue. If cost is an issue, distributed EIDS can be used for critical substation. The distributed EIDS in a hierarchical setting is shown in Figure 6.2. The distributed approach decreases memory requirements, helps reduce EIDS classification time, and enables faster training. The distributed EIDS hierarchical arrangement helps manage the information generated by EIDS and may enable better responses to events. Moreover, the distributed EIDS approach may help to identify the region from where an event started.

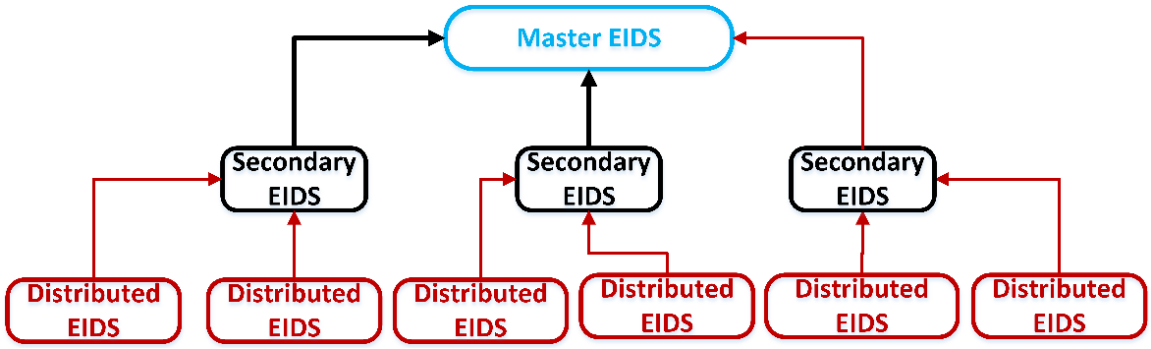


Figure 6.2 Hierarchical approach for EIDS scalability

The criticality of a substation can be defined with index based on size of substation, type of load served, impact on critical services and etc. A number of factors

can be used to define critical substations. Future research on finding critical substations is needed.

The presented EIDS were based on supervised learning. One of the challenges in supervised learning is availability of labels. For real systems, especially for real time operation, label information is not available. Hence, semi-supervised or unsupervised options should be researched.

Finally, in this dissertation, the impact of latency on building EIDS was not studied. Additional research is necessary to address the impact of latency on classification and implementation of the EIDS in real time.

REFERENCES

[1] "Real–Time Application of Synchrophasors for Improving Reliability," NERC, North American Electric Reliability Corporation, Tech. Rep., October 2010.

[2] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, Nov 2011, pp. 4490–4494.

[3] "Final report on the august 14, 2003 blackout in the United States and Canada: Causes and recommendations," U.S.-Canada Power System Outage Task Force, Tech. Rep., April 2004.

[4] "Synchrophasor Technologies and their Deployment in the Recovery Act Smart Grid Programs," U.S. Department of Energy, Tech. Rep., March 2013.

[5] M. Lichman, "UCI machine learning repository," 2013. [Online]. Available: http://archive.ics.uci.edu/ml

[6] A. Bifet and R. Kirkby, *Massive Online Analysis*, August 2009.

[7] E. Bernabeu and F. Katiraie, "Aurora vulnerability." [Online]. Available: https://-www.smartgrid.gov/sites/default/files/doc/files/-Aurora_Vulnerability_Issues_Solution_Hardware_Mitigation_De _201102.pdf

[8] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, "A class of cyber-physical switching attacks for power system disruption," in *Proc. 7th Cyber Security and Information Intelligence Research Workshop (CSIIRW)*, Oak Ridge National Laboratory, Tennessee, October 2011.

[9] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 3, pp. 717–729, March 2014.

[10] T. Kim and H. Poor, "Strategic protection against data injection attacks on power grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 2, pp. 326–333, June 2011.

[11] W. Wang and Z. Lu, "Survey cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[12] S. I. Inc., “Big data meets big data analytics.” [Online]. Available: http://-www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/big-data-meets-big-data-analytics-105777.pdf

[13] K. Sun, S. Likhate, V. Vittal, V. Kolluri, and S. Mandal, “An online dynamic security assessment scheme using phasor measurements and decision trees,” *Power Systems, IEEE Transactions on*, vol. 22, no. 4, pp. 1935–1943, Nov 2007.

[14] E. Voumvoulakis and N. Tziargyriou, “Decision trees-aided self-organized maps for corrective dynamic security,” *IEEE Transactions on Power Systems*, vol. 23, pp. 622–630, 2008.

[15] M. Karthikeyan and V. Malathi, “Wavelet-support vector machine approach for classification of power quality disturbances,” *International Journal of Recent Trends in Engineering*, vol. 1, 2009.

[16] P. Axelberg, I. Gu, and M. Bollen “Support vector machine for classification of volta ge disturbances,” *IEEE Transactions on Power Delivery*, vol. 22, pp. 1297–1303, 2007.

[17] D. Zhou, U. Annakkage, and A. Rajapakse “Online monitoring of voltage stability margin using an ar tificial neural network,” *IEEE Transactions on Power Systems*, vol. 25, pp. 1566–1574, 2010.

[18] D. Novosel and R. King, “Using artificial neural networks for load shedding to alleviate overloaded lines,” *IEEE Transactions on Power Delivery*, vol. 9, pp. 425–433, 1994.

[19] A. Bifet, G. Holmes, R. Kirby and B. Pfahringer. (2011, May) Data stream mining a practical approach.

[20] “Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?” North American Electric Reliability Council, Tech. Rep., July 2004.

[21] “List of major power outages,” http://en.wikipedia.org/wiki /List_of_major_power_outages.

[22] M. Zeller, “Myth or Reality - “Does the Aurora Vulnerability Pose a Risk to My Generator?” Schweitzer Engineering Laboratories, Inc., Tech. Rep., 2011, https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=8504.

[23] D. Salmon, M. Zeller, A. Guzman, V. Mynam, and M. Donolo, “Mitigating the Aurora Vulnerability with Existing Technology,” Schweitzer Engineering Laboratories, Inc., Tech. Rep., September 2009, https://www.selinc.com/WorkArea/DownloadAsset.aspx?id=6379.

[24] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.

[25] R. Bobba, K. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. Overbye, "Detecting false data injection attacks on dc state estimation," in *1st Workshop Secure Control Syst. (CPSWEEK)*, 2010.

[26] S. Liu, "Coordinated variable structure switching attacks for smart grid," Ph.D. dissertation, Department of Electrical and Computer Engineering,Texas A&M University, College Station, TX, 2013.

[27] S. Liu, D. Kundur, T. Zourntos, and K. Butler-Purry, "Coordinated variable structure switching attack in the presence of model error and state estimation," in *Proc. IEEE International Conferenceon Smart Grid Communications (SmartGridComm)*, Taiwan City, Taiwan, November 2012.

[28] National SCADA test bed. [Online]. Available: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

[29] M. McDonald, G. Conrad, T. Service, and R. Cassidy, "Cyber effects analysis using VCSE, promoting control system reliability," Sandia National Laboratory, Tech. Rep., 2008.

[30] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: architecture, application, and evaluation for smart grid," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 847–855, June 2013.

[31] D. Bergman, D. Jin, D. Nicol, and T. Yardley, "The virtual power system testbed and inter-testbed integration," in *Proceedings of the 2Nd Conference on Cyber Security Experimentation and Test*, ser. CSET'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 5–5.

[32] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi, "ICT resilience of power control systems: experimental results from the CRUTIAL testbeds," in *Dependable Systems Networks, 2009. DSN '09. IEEE/IFIP International Conference on*, June 2009, pp. 554–559.

[33] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim-A framework for building SCADA simulations," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 589–597, Dec 2011.

[34] N. Dahal, "Synchrophasor data mining for situational awareness in power systems." Ph.D. dissertation, Mississippi State University, 2012.

[35] C. Zheng, V. Malbasa, and M. Kezunovic, "Regression tree for stability margin prediction using synchrophasor measurements," *Power Systems, IEEE Transactions on*, vol. 28, no. 2, pp. 1978–1987, May 2013.

[36] M. He, V. Vittal, and J. Zhang, "Online dynamic security assessment with missing PMU measurements: A Data Mining Approach," *Power Systems, IEEE Transactions on*, vol. 28, no. 2, pp. 1969–1977, May 2013.

[37] M. He, J. Zhang, and V. Vittal, "Robust online dynamic security assessment using adaptive ensemble decision-tree learning," *Power Systems, IEEE Transactions on*, vol. 28, no. 4, pp. 4089–4098, Nov 2013.

[38] S. Pan, "Cybersecurity testing and intrusion detection for cyber-physical power systems," Ph.D. dissertation, Mississippi State University, December 2014.

[39] A. Bifet, "Adaptive learning and mining for data streams and frequent patterns," Ph.D. dissertation, Universitat Polit'ecnica de Catalunya, April 2009.

[40] A. Guzman, S. Samineni, and M. Bryson, "Protective relay synchrophasor measurements during fault conditions," in *Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2006. PS '06*, March 2006, pp. 83–95.

[41] P. Kundur, "Power System Stability and Control," 1994.

[42] "RTDS Technologies," http://www.rtds.com/applications/applications.html.

[43] T. Morris, S. Pan, U. Adhikari, N. Younan, R. King, and V. Madani "Cyber security testing and intrusion detection for synchrophasor systems," *International Journal of Network Science (IJNS). Inderscience*, in press.

[44] H. Saadat, *Power System Analysis*. PSA Publishing, 2010.

[45] H. Ferrer, E. Schweitzer, and S. E. Laboratories, *Modern Solutions for Protection, Control, and Monitoring of Electric Power Systems*. Schweitzer Engineering Laboratories, Incorporated, 2010.

[46] M. Chen, "Dynamic contingency re-definition in power system security analysis," in *Electric Utility Deregulation and Restructuring and Power Technologies (DRPT), 2011 4th International Conference on*, July 2011, pp. 63–66.

[47] G. Weimann and U. S. I. of Peace, *Cyberterrorism: how real is the threat?* UCI Special report. United States Institute of Peace, 2004, no. v. 31, nos. 20-119.

[48] The UCI KDD archive. University of California, Department of Information and Computer Science. Irvine, CA. [Online]. Available: http://kdd.ics.uci.edu

[49] R. Hink, J. Beaver, M. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *Resilient Control Systems (ISRCS), 2014 7th International Symposium on*, Aug 2014, pp. 1–8.

[50] N. Dahal, R. King, and V. Madani, "Online dimension reduction of synchrophasor data," in *Transmission and Distribution Conference and Exposition (T D), 2012 IEEE PES*, May 2012, pp. 1–7.

[51] U. Adhikari, T. Morris, N. Dahal, S. Pan, R. King, N. Younan, and V. Madani, "Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in RTDS," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–7.

[52] T. Morris, S. Pan, and U. Adhikari, "Cyber security recommendations for wide area monitoring, protection, and control systems," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–6.

[53] T. Morris and S. Pan and U. Adhikari and N. Younan and R. King and V. Madani, *Phasor Measurement Unit and Phasor Data Concentrator Cyber Security*. Springer Berlin Heidelberg, 2013, 978-3-642-38133-1.

[54] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 235–244, March 2013.

[55] I. Witten, E. Frank, and M. Hall, *Data Mining: Practical Machine Learning Tools and Techniques: Practical Machine Learning Tools and Techniques*, ser. The Morgan Kaufmann Series in Data Management Systems. Elsevier Science, 2011. [Online]. Available: https://books.google.ae/books?id=bDtLM8CODsQC

[56] P. Trachian, "Machine learning and windowed subsecond event detection on PMU data via hadoop and the OpenPDC," in *Power and Energy Society General Meeting, 2010 IEEE*, July 2010, pp. 1–5.

[57] J. Ye, Q. Li, H. Xiong, H. Park, R. Janardan, and V. Kumar, "Idr/qr: an incremental dimension reduction algorithm via qr decomposition," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 17, no. 9, pp. 1208–1222, Sept 2005.

[58] M. Ye, X. Li, and M. Orlowska, "Supervised dimensionality reduction on streaming data," in *Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on*, vol. 1, Aug 2007, pp. 674–678.

[59] L. Xie, Y. Chen, and P. Kumar, "Dimensionality reduction of synchrophasor data for early event detection: Linearized analysis," *Power Systems, IEEE Transactions on*, vol. 29, no. 6, pp. 2784–2794, Nov 2014.

[60] Y. Chen and B. Luo, "S2a: Secure smart household appliances," in *Proceedings of the Second ACM Conference on Data and Application Security and Privacy*, ser. CODASPY '12. New York, NY, USA: ACM, 2012, pp. 217–228. [Online]. Available: http://doi.acm.org/10.1145/2133601.2133628

[61] Z. Wang, Y. Zhang, and J. Zhang, "Principal components fault location based on WAMS/PMU measure system," in *Power and Energy Society General Meeting, 2011 IEEE*, July 2011, pp. 1–5.

[62] J. Yan, B. Zhang, S. Yan, N. Liu, Q. Yang, Q. Cheng, H. Li, Z. Chen, and W. Ma, "A scalable supervised algorithm for dimensionality reduction on streaming data," *Information Sciences*, vol. 176, no. 14, pp. 2042 – 2065, 2006, streaming Data Mining. [Online]. Available: http://www.sciencedirect.com/science/article/pii/-S0020025505003063

[63] S. Horowitz and A. Phadke, *Power System Relaying*, ser. RSP. Wiley, 2008. [Online]. Available: https://books.google.com/books?id=4A3Kw3fgNusC

[64] J. Glover, M. Sarma, and T. Overbye, *Power System Analysis & Design, SI Version*. Cengage Learning, 2011. [Online]. Available: https://books.google.com/-books?id=XScJAAAAQBAJ

[65] "Frequency response standard whitepaper," NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL, Tech. Rep., April 2004.

[66] I. Kamwa, S. Samantaray, and G. Joos, "Development of rule-based classifiers for rapid stability assessment of wide-area post-disturbance records," *Power Systems, IEEE Transactions on*, vol. 24, no. 1, pp. 258–270, Feb 2009.

[67] G. Holmes, R. Kirby, and B. Pfahringer, "Batch-incremental learning for mining data streams," University of Waikato, Tech. Rep.

[68] B. Martin, "Instance-based learning: Nearest neighbour with generalisation," Master's thesis, University of Waikato, Hamilton, Neq Zealand, March 1995.

[69] M. Al Karim, M. Chenine, K. Zhu, and L. Nordstrom, "Synchrophasor-based data mining for power system fault analysis," in *Innovative Smart Grid Technologies (ISGT Europe), 2012 3rd IEEE PES International Conference and Exhibition on*, Oct 2012, pp. 1–8.

[70] O. Dahal, S. Brahma, and H. Cao, "Comprehensive clustering of disturbance events recorded by phasor measurement units," *Power Delivery, IEEE Transactions on*, vol. 29, no. 3, pp. 1390–1397, June 2014.

[71] O. Dahal, H. Cao, S. Brahma, and R. Kavasseri, "Evaluating performance of classifiers for supervisory protection using disturbance data from phasor measurement units," in *Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES*, Oct 2014, pp. 1–6.

[72] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan, and H. Wang, "Intrusion detection system for network security in synchrophasor systems," in *Information and Communications Technologies (IETICT 2013), IET International Conference on*, April 2013, pp. 246–252.

[73] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 796–808, Dec 2011.

[74] H. Hadeli, R. Schierholz, M. Braendle, and C. Tuduce, "Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration," in *Emerging Technologies Factory Automation, 2009. ETFA 2009. IEEE Conference on*, Sept 2009, pp. 1–8.

[75] R. Berthier and W. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on*, Dec 2011, pp. 184–193.

[76] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *Power Systems, IEEE Transactions on*, vol. 28, no. 2, pp. 1052–1062, May 2013.

[77] J. Morteza Talebi and Z. Qu, "Secure power systems against malicious cyber-physical data attacks: Protection and identification," *World Academy of Science, Engineering and Technology*, vol. 6, 2012.

[78] R. Bouckaert, E. Frank, M. Hall, R. Kirby, P. Reutemann, A. Seewald, and D. Scuse, *WEKA Manual for Version 3-7-8*, January 2013.

[79] A. Bifet and E. Frank, "Sentiment knowledge discovery in twitter streaming data," in *Proceedings of the 13th International Conference on Discovery Science*, ser. DS'10. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 1–15. [Online]. Available: http://dl.acm.org/citation.cfm?id=1927300.1927301

[80] A. Bifet and B. Pfahringer, "Improving adaptive bagging methods for evolving data streams," in *In ACML*, 2009, pp. 23–37.

[81] A. Bifet, G. Holmes, B. Pfahringer, R. Kirkby, and R. Gavaldà, "New ensemble methods for evolving data streams," in *Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD '09. New York, NY, USA: ACM, 2009, pp. 139–148. [Online]. Available: http://-doi.acm.org/10.1145/1557019.1557041

[82] A. Bifet and R. Gavaldà, “Adaptive parameter-free learning from evolving data streams.”

[83] A. Bahga and V. Madisetti, “Analyzing massive machine maintenance data in a computing cloud,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 10, pp. 1831–1843, Oct 2012.

[84] J. Gama and P. Rodrigues, “EnglishStream-based electricity load forecast,” in *EnglishKnowledge Discovery in Databases: PKDD 2007*, Lecture Notes in Computer Science, J. Kok, J. Koronacki, R. Lopez de Mantaras, S. Matwin, D. MladeniÄ?, and A. Skowron, Eds. Springer Berlin Heidelberg, 2007, vol. 4702, pp. 446–453. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74976-9_45

[85] M. Faisal, Z. Aung, J. Williams, and A. Sanchez, “Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study,” *Systems Journal, IEEE*, vol. 9, no. 1, pp. 31–44, March 2015.

[86] J. Gama, P. Medas, G. Castillo, and P. Rodrigues, “Learning with drift detection,” in *In SBIA Brazilian Symposium on Artificial Intelligence*. Springer Verlag, 2004, pp. 286–295.

[87] P. Domingos and G. Hulten, “Mining high-speed data streams,” in *Proceedings of the Sixth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ser. KDD ’00. New York, NY, USA: ACM, 2000, pp. 71–80. [Online]. Available: http://doi.acm.org/10.1145/347090.347107

[88] R. Mitchell and I. Chen, “Behavior-rule based intrusion detection systems for safety critical smart grid applications,” *Smart Grid, IEEE Transactions on*, vol. 4, no. 3, pp. 1254–1263, Sept 2013.

[89] I. Zliobaite , A. Bifet , G. Holmes and B. Pfahringer "MOA concept drift active learning strategies for streaming data", *Proc. 2nd Workshop Appl. Pattern Anal.*, vol. 17, pp.48 -55 2011

APPENDIX A

SCENARIOS FOR DATASETS

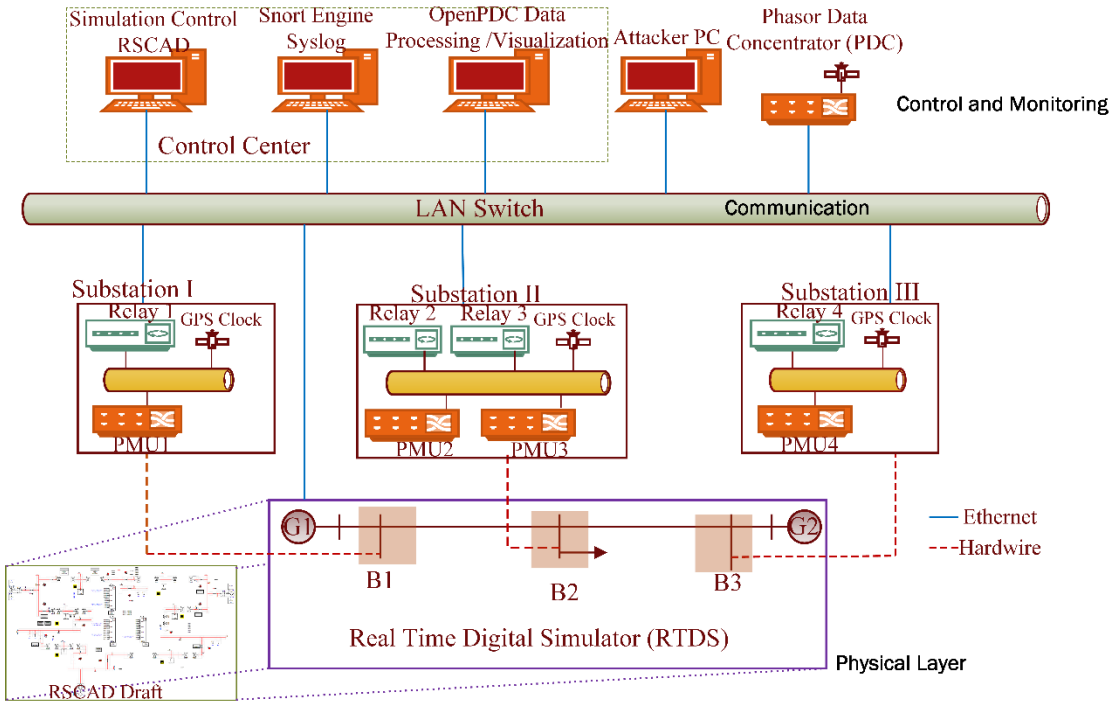


Figure A.1 WAMS implementation of three bus two generator system

Table A.2 Scenario list with associated single line diagram and expected relay state

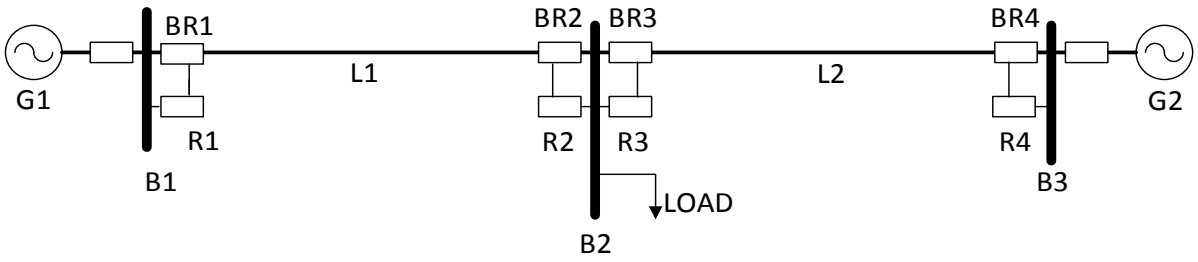
ID	Scenarios Descriptions	Relay R1	Relay R2	Relay R3	Relay R4
					
	Note: *Each relay has Zone 1 from 10% to 80% and Zone 2 from 80% to 150% of the line.*				
	Legend: **I**: *Instant Tripping for Zone 1 protection*; **TD**: *Time Delayed Tripping for Zone 2 protection*; **N**: *Normal*; **NR**: *No Response.*				
	*Categories marked with * are attacks. Category I and II is a pair. Category III and IV is another pair. Category V are attacks that interrupt the relay operations.*				
	2% scenarios are nothing happen				
	Primary protection properly working 20%				
Q1	SLG Fault at 10% - 19% on line L1	I	TD	N	N
Q2	SLG Fault at 20% - 79% on line L1	I	I	N	N
Q3	SLG Fault at 80% - 90% on line L1	TD	I	N	N
Q4	SLG Fault at 10% - 19% on line L2	N	N	I	TD
Q5	SLG Fault at 20% - 79% on line L2	N	N	I	I
Q6	SLG Fault at 80% - 90% on line L2	N	N	TD	I
	***SLG Fault replay (This category will be the repeat of category I except there are tripping command detected.) 14%**				
Q7	SLG Fault at 10% - 19% on line L1	I	TD	N	N
Q8	SLG Fault at 20% - 79% on line L1	I	I	N	N
Q9	SLG Fault at 80% - 90% on line L1	TD	I	N	N
Q10	SLG Fault at 10% - 19% on line L2	N	N	I	TD
Q11	SLG Fault at 20% - 79% on line L2	N	N	I	I
Q12	SLG Fault at 80% - 90% on line L2	N	N	TD	I
	Line maintenance 5%				
	III.1 Line maintenance only				
Q13	Line L1 maintenance	Trip	Trip	N	N
Q14	Line L2 maintenance	N	N	Trip	Trip
	***Command (CMD) injection against single relay 8%**				
Q15	CMD Injection to R1	Trip	N	N	N
Q16	CMD Injection to R2	N	Trip	N	N
Q17	CMD Injection to R3	N	N	Trip	N
Q18	CMD Injection to R4	N	N	N	Trip
	***Command (CMD) injection against two relays 5%**				
Q19	CMD Injection to R1 & R2	Trip	Trip	N	N
Q20	CMD Injection to R3 & R4	N	N	Trip	Trip
	***Primary protection disabled towards single relay 23%**				
	VI.1 Single relay disabled & SLG Fault 18%				
	VI.1.1 R1 disabled & SLG Fault				
Q21	SLG Fault at 10% - 19% on line L1	NR	TD	N	N
Q22	SLG Fault at 20% - 90% on line L1	NR	I	N	N
	VI.1.2 R2 disabled & SLG Fault				
Q23	SLG Fault at 10% - 49% on line L1	I	NR	N	N
Q24	SLG Fault at 50% - 79% on line L1	I	NR	N	TD
Q25	SLG Fault at 80% - 90% on line L1	TD	NR	N	TD
	VI.1.3 R3 disabled & SLG Fault				
Q26	SLG Fault at 10% - 19% on line L2	TD	N	NR	TD
Q27	SLG Fault at 20% - 49% on line L2	TD	N	NR	I
Q28	SLG Fault at 50% - 90% on line L2	N	N	NR	I
	VI.1.4 R4 disabled & SLG Fault				
Q29	SLG Fault at 10% - 79% on line L2	N	N	I	NR
Q30	SLG Fault at 80% - 90% on line L2	N	N	TD	NR

Table A.2 (Continued)

VI.2 Single relay disabled & line maintenance 5%					
VI.2.1 R1 disabled & L1 maintenance					
Q31	L1 Maintenance	NR	Trip	N	N
VI.2.2 R2 disabled & L1 maintenance					
Q32	L1 Maintenance	Trip	NR	N	N
VI.2.3 R3 disabled & L2 maintenance					
Q33	L2 Maintenance	N	N	NR	Trip
VI.2.4 R4 disabled & L2 maintenance					
Q34	L2 Maintenance	N	N	Trip	NR
***Primary protection disabled towards two relays 23%**					
VII.1 Two relay disabled & SLG Fault 18%					
VII.1.1 R1 & R2 disabled & SLG Fault					
Q35	SLG Fault at 10% - 49% on line L1	NR	NR	N	N
Q36	SLG Fault at 50% - 90% on line L1	NR	NR	N	TD
VII.1.2 R3 & R4 disabled & SLG Fault					
Q37	SLG Fault at 10% - 49% on line L2	TD	N	NR	NR
Q38	SLG Fault at 50% - 90% on line L2	N	N	NR	NR
VII.2 Two relay disabled & Line maintenance 5%					
VII.2.1 R1 & R2 disabled & L1 maintenance					
Q39	L1 Maintenance	NR	NR	N	N
VII.2.2 R3 & R4 disabled & L2 maintenance					
Q40	L2 Maintenance	N	N	NR	NR
Q41	No events normal operation				
These are new scenarios					
Primary protection properly working for Line to line faults 28%					
Q102	LL Fault at 10% - 19% on line L1	I	TD	N	N
	LL Fault at 20% - 79% on line L1	I	I	N	N
	LL Fault at 80% - 90% on line L1	TD	I	N	N
	LL Fault at 10% - 19% on line L2	N	N	I	TD
	LL Fault at 20% - 79% on line L2	N	N	I	I
	LL Fault at 80% - 90% on line L2	N	N	TD	I
Primary protection properly working for 2 Lines to ground faults 28%					
Q108	2LG Fault at 10% - 19% on line L1	I	TD	N	N
	2LG Fault at 20% - 79% on line L1	I	I	N	N
	2LG Fault at 80% - 90% on line L1	TD	I	N	N
	2LG Fault at 10% - 19% on line L2	N	N	I	TD
	2LG Fault at 20% - 79% on line L2	N	N	I	I
	2LG Fault at 80% - 90% on line L2	N	N	TD	I
Primary protection properly working for 3 Lines to ground faults 28%					
Q114	3LG Fault at 10% - 19% on line L1	I	TD	N	N
	3LG Fault at 20% - 79% on line L1	I	I	N	N
	3LG Fault at 80% - 90% on line L1	TD	I	N	N
	3LG Fault at 10% - 19% on line L2	N	N	I	TD
	3LG Fault at 20% - 79% on line L2	N	N	I	I
	3LG Fault at 80% - 90% on line L2	N	N	TD	I
Aurora 16%					
Q119	CMD Injection to R1	Trip	N	N	N

APPENDIX B

CONFUSION MATRICES FOR EXPERIMENTS IN CHAPTER 4

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	
368	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
19	261	37	0	0	0	4	3	0	0	0	0	0	0	0	0	0	0	3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q2
0	20	322	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	306	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	Q4
0	0	0	33	271	4	0	0	0	0	13	13	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	Q5
0	0	0	0	5	356	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	Q6
0	5	0	0	0	0	202	29	2	0	0	0	3	0	0	0	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	Q7
0	9	0	0	0	0	52	125	31	0	0	0	3	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	Q8
0	0	0	0	0	0	3	13	211	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q9
0	0	0	0	1	0	0	0	0	205	15	7	0	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	Q10
0	0	0	0	12	0	0	0	0	31	105	71	0	6	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	2	2	0	0	Q11
0	0	0	0	14	0	0	0	0	7	43	158	0	8	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	259	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	0	0	233	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	1	0	0	0	0	0	0	0	0	198	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	194	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	187	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q18
0	0	0	0	0	0	1	0	12	0	0	0	6	0	0	0	0	0	258	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	1	0	0	0	0	7	22	19	0	9	0	0	0	0	0	204	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	174	22	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q21
0	2	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	21	183	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	198	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	157	27	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	Q24
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20	171	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	174	19	0	0	0	0	0	0	0	0	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	16	164	2	0	0	0	0	0	0	0	2	0	0	0	0	Q27
0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	195	0	0	0	0	0	0	0	0	0	0	0	0	Q28
0	0	0	12	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	152	22	0	0	0	0	0	0	1	0	0	0	Q29
0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	20	204	0	0	0	0	0	0	3	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	79	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	86	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	54	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	Q34
0	0	0	0	0	0	38	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	432	3	0	0	0	0	Q35
0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	458	0	0	0	0	Q36
1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	472	1	0	0	Q37
0	0	0	0	0	0	0	0	0	0	19	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	3	413	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	26	0	0	0	0	0	0	0	127	1	Q39
0	0	0	0	0	2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	247	Q40

Figure B.1 Experiment 1, Case 1

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
359	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q1
23	279	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q2
0	30	322	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	260	62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	1	0	0	0	0	0	Q4
0	0	0	29	295	1	0	1	1	4	8	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q5
0	0	0	0	1	360	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0	0	1	Q6
0	0	0	0	0	0	222	17	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	Q7
0	1	0	0	0	58	92	67	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	Q8
0	0	0	0	0	0	4	58	160	0	0	0	6	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	Q9
0	0	0	0	4	0	0	0	0	144	59	17	0	7	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	4	0	0	0	0	77	82	60	0	5	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	Q11
0	0	0	0	8	0	0	0	0	19	39	163	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	260	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	2	0	232	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	194	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	194	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	0	3	0	0	0	3	0	0	0	0	0	0	271	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	2	2	0	0	1	0	0	0	0	0	0	257	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	195	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q21
0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	198	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	Q22
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	198	9	0	0	0	0	0	0	0	0	0	1	0	2	0	0	0	0	Q23
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	21	132	32	3	0	0	0	0	0	0	0	1	0	4	0	0	0	0	Q24
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	22	141	27	5	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	25	130	42	0	0	0	0	0	0	1	1	0	0	0	0	0	Q26
0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	40	136	0	0	0	0	0	0	0	1	0	0	0	0	0	Q27
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	203	0	1	0	0	0	0	0	0	0	0	0	0	Q28
0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	176	8	0	0	0	0	0	0	1	0	0	0	Q29
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	9	215	0	0	0	0	0	1	1	2	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	83	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	86	0	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	Q34
0	0	0	0	0	0	17	12	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	443	1	3	2	0	0	0	Q35
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	4	455	1	1	0	0	1	Q36
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2	0	470	2	0	0	0	Q37
0	0	0	0	0	0	0	0	0	0	7	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	433	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	50	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	26	0	0	0	0	0	0	0	179	1	0	Q39
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	251	0	Q40
1	0	0	0	1	29	2	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4	0	0	0	0	0	0	0	3	0	9	6	0	0	164	Q41

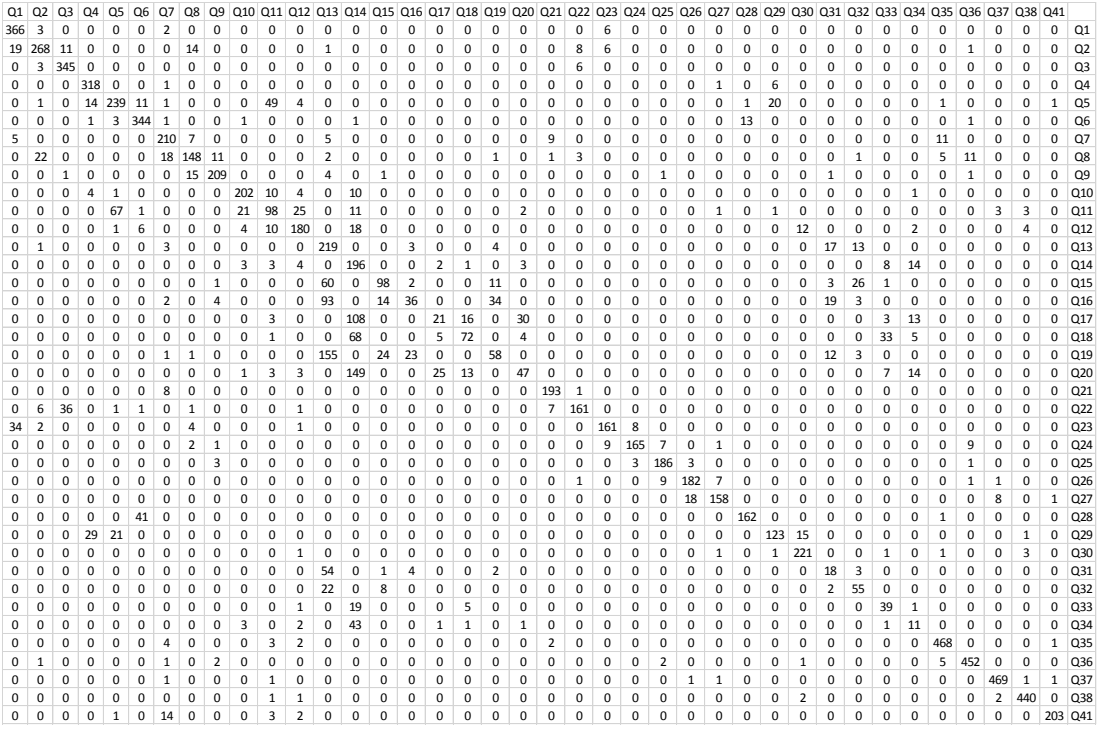
Figure B.2 Experiment 1, Case 2

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
367	8	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
22	272	22	0	0	0	0	8	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	Q2
0	17	332	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	293	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	Q4
0	0	0	26	274	6	0	0	0	5	24	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	Q5
0	0	0	0	5	352	0	0	0	0	0	4	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	Q6
1	0	0	0	0	0	219	16	3	0	0	0	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	Q7
0	2	0	0	0	0	37	133	40	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	2	0	1	0	0	0	0	Q8
0	1	0	0	0	0	1	40	183	0	0	0	1	0	0	0	0	0	4	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q9
0	0	0	0	4	0	0	0	0	172	48	5	0	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	11	0	0	0	0	61	91	59	0	3	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3	0	0	0	0	Q11
0	0	0	0	6	1	0	0	0	12	30	174	0	3	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	259	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	1	0	0	0	232	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	184	0	0	0	17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	187	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	266	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	1	3	3	0	6	0	0	0	0	0	249	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	192	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q21
0	0	19	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	2	192	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	186	16	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	Q23
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	150	16	4	1	0	0	0	0	0	0	1	2	4	0	0	0	0	0	Q24
0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	134	30	5	0	0	0	0	0	0	0	3	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	27	139	19	0	0	0	0	0	0	0	0	2	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	4	33	143	0	0	0	0	0	0	0	0	2	0	0	0	0	0	Q27
0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	7	184	0	0	0	0	0	0	0	5	0	0	0	0	0	Q28
0	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	166	10	0	0	0	0	0	0	1	0	0	0	0	Q29
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	217	0	0	0	0	0	1	0	2	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	82	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	84	0	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	Q34
0	0	0	0	0	0	15	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	460	1	0	0	0	0	0	Q35
0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	5	0	5	7	0	0	0	0	0	0	3	438	0	1	0	0	0	Q36
2	1	0	0	0	0	1	1	5	0	0	0	0	0	0	0	0	0	0	0	0	0	6	7	0	0	0	0	0	0	0	0	0	0	0	0	450	2	0	0	0	Q37
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	444	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	25	1	0	0	0	0	0	0	102	0	0	Q39
0	0	0	0	0	2	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	Q40
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	79	Q41

Figure B.3 Experiment 1, Case 3

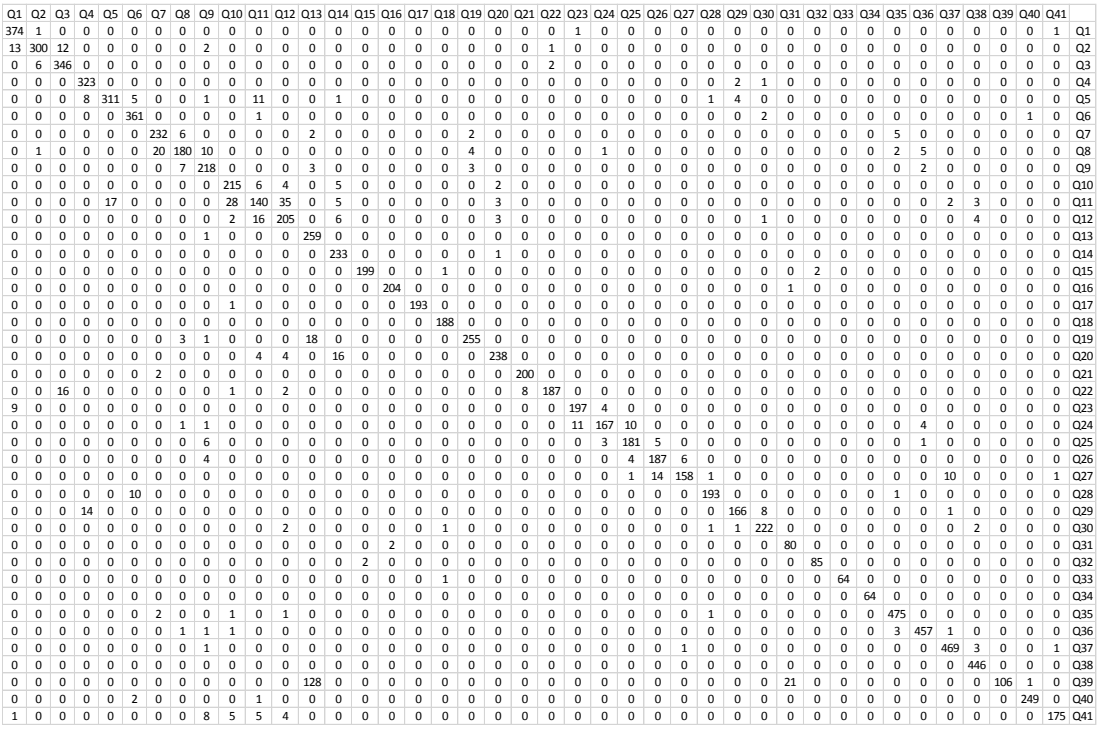
Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	
360	13	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
13	300	9	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q2
0	10	342	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	321	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	Q4
0	0	0	10	319	4	0	0	0	5	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	Q5
0	0	0	0	2	360	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	Q6
0	2	0	0	0	0	213	25	0	0	0	0	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	Q7
0	4	0	0	0	0	20	186	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	3	1	0	0	0	0	0	Q8
0	0	0	0	0	0	1	5	222	0	0	0	2	0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q9
0	0	0	0	1	0	0	0	0	214	13	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	11	0	0	0	0	23	154	36	0	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	3	2	0	0	0	Q11
0	0	0	0	5	0	0	0	0	4	23	198	0	2	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	257	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	1	0	232	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	Q14
0	0	0	0	0	1	0	0	0	0	0	0	0	0	195	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	37	0	10	0	0	0	0	147	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	187	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	2	0	7	0	0	0	3	0	0	0	0	0	265	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	43	29	50	0	0	0	0	0	0	0	140	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	185	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q21
0	1	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	202	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	200	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	7	175	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q24
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	178	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	169	23	0	0	0	0	0	0	0	0	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	16	167	0	0	0	0	0	0	0	0	2	0	0	0	0	Q27
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	201	0	0	0	0	0	0	0	0	0	0	0	0	Q28
0	0	0	3	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	171	13	0	0	0	0	0	0	0	0	0	0	Q29
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	8	216	0	0	0	0	0	0	4	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	82	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	86	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	Q34
0	0	0	0	0	0	19	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	446	4	0	0	0	0	Q35
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	458	0	0	0	0	0	Q36
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	1	0	0	0	469	1	0	0	0	Q37
0	0	0	0	0	0	0	0	0	0	8	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	435	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	71	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	54	0	0	0	0	0	0	0	131	0	Q39
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	251	Q40

Figure B.4 Experiment 1, Case 4



Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q41	
366	3	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
19	268	11	0	0	0	0	14	0	0	0	0	1	0	0	0	0	0	0	0	0	8	6	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	Q2
0	3	345	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	318	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	6	0	0	0	0	0	0	0	0	0	Q4
0	1	0	14	239	11	1	0	0	0	49	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	20	0	0	0	0	0	1	0	0	1	Q5
0	0	0	1	3	344	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	13	0	0	0	0	0	0	1	0	0	0	Q6
5	0	0	0	0	0	210	7	0	0	0	0	5	0	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	11	0	0	0	0	Q7
0	22	0	0	0	0	18	148	11	0	0	0	2	0	0	0	0	0	1	0	1	3	0	0	0	0	0	0	0	0	0	1	0	0	5	11	0	0	Q8
0	0	1	0	0	0	0	15	209	0	0	0	4	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	Q9
0	0	0	4	1	0	0	0	0	202	10	4	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	Q10
0	0	0	0	67	1	0	0	0	21	98	25	0	11	0	0	0	0	0	2	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	3	3	0	Q11
0	0	0	1	6	0	0	0	4	10	180	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	2	0	0	4	0	Q12
0	1	0	0	0	0	3	0	0	0	0	0	219	0	0	3	0	0	4	0	0	0	0	0	0	0	0	0	0	0	17	13	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	3	3	4	0	196	0	0	2	1	0	3	0	0	0	0	0	0	0	0	0	0	0	8	14	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	1	0	0	0	60	0	98	2	0	0	11	0	0	0	0	0	0	0	0	0	0	3	26	1	0	0	0	0	0	0	Q15
0	0	0	0	0	0	2	0	4	0	0	0	93	0	14	36	0	0	34	0	0	0	0	0	0	0	0	0	0	19	3	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	0	3	0	0	108	0	0	21	16	0	30	0	0	0	0	0	0	0	0	0	0	0	3	13	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	1	0	0	68	0	0	5	72	0	4	0	0	0	0	0	0	0	0	0	0	0	33	5	0	0	0	0	0	Q18
0	0	0	0	0	0	1	1	0	0	0	0	155	0	24	23	0	0	58	0	0	0	0	0	0	0	0	0	0	12	3	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	1	3	3	0	149	0	0	25	13	0	47	0	0	0	0	0	0	0	0	0	0	0	7	14	0	0	0	0	0	Q20
0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	193	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q21
0	6	36	0	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	7	161	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
34	2	0	0	0	0	4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	161	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	9	165	7	0	1	0	0	0	0	0	0	0	9	0	0	0	Q24
0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	186	3	0	0	0	0	0	0	0	0	1	0	0	0	Q25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	9	182	7	0	0	0	0	0	0	0	1	1	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	18	158	0	0	0	0	0	0	0	8	0	1	Q27
0	0	0	0	41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	162	0	0	0	0	0	1	0	0	0	0	Q28
0	0	0	29	21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	123	15	0	0	0	0	0	0	1	0	Q29
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	221	0	0	1	0	1	0	0	3	Q30
0	0	0	0	0	0	0	0	0	0	0	0	54	0	1	4	0	0	2	0	0	0	0	0	0	0	0	0	0	0	18	3	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	22	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	55	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	1	0	19	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	39	1	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	3	0	2	0	43	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	11	0	0	0	0	0	Q34
0	0	0	0	0	0	4	0	0	0	3	2	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	468	0	0	0	1	Q35
0	1	0	0	0	0	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	5	452	0	0	Q36
0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	469	1	Q37
0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	440	0	Q38
0	0	0	0	1	0	14	0	0	0	3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	203	Q41

Figure B.5 Experiment 1, Case 5



Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
374	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	Q1
13	300	12	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q2
0	6	346	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	323	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	Q4
0	0	0	8	311	5	0	0	1	0	11	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	4	0	0	0	0	0	0	0	0	0	0	0	0	Q5
0	0	0	0	0	361	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	1	0	Q6
0	0	0	0	0	0	232	6	0	0	0	0	2	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	Q7
0	1	0	0	0	0	20	180	10	0	0	0	0	0	0	0	0	0	4	0	0	0	0	1	0	0	0	0	0	0	0	0	2	5	0	0	0	0	0	0	Q8
0	0	0	0	0	0	0	7	218	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	Q9
0	0	0	0	0	0	0	0	0	215	6	4	0	5	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	17	0	0	0	0	28	140	35	0	5	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	3	0	0	0	Q11
0	0	0	0	0	0	0	0	0	2	16	205	0	6	0	0	0	0	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0	4	0	0	0	0	Q12
0	0	0	0	0	0	0	0	1	0	0	0	259	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	199	0	0	1	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	204	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	0	3	1	0	0	0	18	0	0	0	0	0	255	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	4	4	0	16	0	0	0	0	0	0	238	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q21
0	0	16	0	0	0	0	0	0	1	0	2	0	0	0	0	0	0	0	0	8	187	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	197	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	11	167	10	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	Q24
0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	3	181	5	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	187	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	14	158	1	0	0	0	0	0	0	0	10	0	0	0	1	0	Q27
0	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	193	0	0	0	0	0	0	1	0	0	0	0	0	0	Q28
0	0	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	166	8	0	0	0	0	0	1	0	0	0	0	0	Q29
0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	222	0	0	0	0	0	0	2	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	85	0	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	Q34
0	0	0	0	0	2	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	475	0	0	0	0	0	0	Q35
0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	457	1	0	0	0	0	Q36
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	469	3	0	0	1	Q37
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	446	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	21	0	0	0	0	0	0	0	106	1	0	Q39
0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	249	0	Q40
1	0	0	0	0	0	0	0	8	5	5	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	175	Q41

Figure B.6 Experiment 2, Case 1

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
331	2	1	1	0	6	5	6	1	8	0	0	1	0	0	0	0	5	0	0	0	2	0	0	0	1	0	0	1	0	0	0	0	0	0	1	3	0	0	1	Q1
18	261	13	1	0	1	4	6	2	2	4	4	1	1	0	0	0	0	0	1	0	2	0	0	1	0	1	0	0	0	0	0	0	0	0	2	1	0	0	0	2	Q2
0	5	308	2	0	2	6	4	2	1	5	1	0	0	0	0	0	1	3	0	0	2	2	0	0	0	1	0	1	2	0	0	0	0	0	0	3	0	0	0	3	Q3
1	2	2	292	0	0	1	4	3	6	3	1	0	0	0	0	0	0	2	0	1	0	2	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	1	2	Q4
2	1	4	14	261	4	4	3	7	0	18	6	1	0	0	0	0	0	3	0	0	0	2	0	0	0	0	0	8	1	0	0	0	0	0	1	0	0	1	0	1	Q5
1	5	4	2	2	315	3	7	2	1	6	1	0	0	0	0	0	1	1	1	0	0	2	0	0	0	0	1	1	2	0	0	0	0	0	0	0	0	1	3	3	Q6
0	0	0	0	0	0	215	5	3	3	2	4	1	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	10	0	0	0	1	0	0	Q7
0	0	0	0	0	0	25	142	16	3	0	7	0	2	0	0	0	0	4	0	0	0	0	3	0	0	0	0	0	0	0	0	0	3	15	0	0	3	0	0	0	Q8
0	0	0	0	0	0	5	7	200	1	0	7	0	0	0	0	0	0	4	0	0	0	0	0	3	0	0	0	0	0	0	1	0	0	0	2	1	0	1	1	0	Q9
0	0	0	0	0	0	5	4	1	184	8	14	0	5	0	0	0	0	0	2	0	0	0	0	0	4	0	0	1	0	0	0	1	1	0	0	0	0	1	0	1	Q10
0	0	0	0	23	0	4	5	3	27	123	25	0	7	0	0	0	0	0	4	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	5	4	0	1	0	Q11
0	0	0	0	3	0	1	5	2	9	16	175	0	13	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	2	0	0	Q12
0	0	0	0	0	0	3	0	1	0	0	0	234	7	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	8	3	0	0	Q13
0	0	0	0	0	0	1	0	2	0	0	1	2	216	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	6	0	0	0	Q14
1	1	1	0	1	1	0	4	3	0	3	1	0	0	175	0	0	0	1	0	1	0	2	0	0	0	1	0	0	0	1	2	0	0	0	0	2	0	0	0	1	Q15
0	2	0	2	0	0	2	1	3	0	2	0	0	0	0	180	0	0	2	1	0	0	1	0	0	0	0	1	1	2	1	0	0	0	0	0	2	0	0	0	2	Q16
0	2	2	0	0	0	4	0	3	2	4	3	0	0	0	0	169	0	2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	1	Q17
0	2	4	0	3	0	1	1	2	2	2	2	0	0	0	0	0	160	2	0	0	0	1	0	0	0	0	2	0	2	0	0	0	0	0	0	2	0	0	0	0	Q18
0	4	5	0	1	0	8	1	1	0	5	2	17	0	0	1	0	0	226	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	1	Q19
0	0	4	0	1	0	4	4	2	2	3	4	0	27	0	0	0	0	3	199	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	2	0	0	0	2	Q20
0	4	1	0	0	0	6	2	3	0	5	1	0	0	0	0	1	0	0	0	171	0	1	0	1	0	0	1	1	1	0	0	0	0	2	0	1	0	0	0	0	Q21
0	8	26	1	0	1	2	2	2	0	1	2	0	1	0	0	0	0	0	0	0	9	151	2	0	1	0	0	1	0	0	0	0	0	0	0	2	0	0	1	1	Q22
19	2	2	1	0	0	2	3	1	1	4	2	0	0	0	0	0	0	0	3	0	0	1	161	6	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	Q23
0	3	0	1	0	0	5	3	1	0	6	2	1	0	0	0	0	0	0	0	0	0	0	9	145	5	1	0	0	0	0	0	0	0	0	10	1	0	0	0	1	Q24
1	2	0	0	0	0	2	1	11	0	2	0	0	0	0	0	0	0	1	0	2	0	0	1	163	1	1	0	1	0	0	0	0	0	0	5	1	0	0	0	1	Q25
0	2	2	0	0	0	4	3	1	2	4	1	0	0	0	0	0	0	2	0	0	0	1	1	2	167	2	2	0	0	0	0	0	0	0	1	4	0	0	0	0	Q26
0	2	0	2	0	0	2	2	2	0	4	2	0	0	0	0	0	0	0	0	0	0	0	2	0	1	11	133	4	0	1	0	0	0	0	0	16	0	1	0	0	Q27
1	3	4	0	0	23	4	2	1	1	4	0	0	1	0	0	0	1	0	0	0	0	0	4	0	0	0	1	148	0	2	0	0	0	0	0	2	1	0	1	0	Q28
0	6	1	24	6	0	1	2	2	0	5	1	0	0	0	0	0	0	1	0	0	0	0	4	0	0	0	1	0	118	11	0	0	0	1	0	1	3	1	0	0	0	Q29
0	2	1	0	0	1	3	1	1	2	3	2	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	2	202	0	0	0	0	0	2	1	2	0	0	2	Q30
0	0	0	0	0	0	1	0	0	2	0	1	7	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	65	0	0	0	0	0	0	4	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	2	5	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	72	0	0	0	0	0	2	2	0	0	Q32
0	0	0	0	0	0	0	0	1	0	0	1	1	3	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	52	0	0	0	0	0	2	0	0	Q33
0	0	0	0	0	0	0	0	0	1	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	58	0	0	0	0	0	0	0	Q34
0	5	3	0	1	0	9	4	8	0	11	8	0	0	0	0	1	0	7	0	2	2	3	0	0	0	0	1	1	1	0	0	0	0	404	3	3	0	0	1	2	Q35
0	8	1	1	1	1	6	7	4	1	7	1	1	0	0	1	1	0	1	0	0	0	3	1	8	0	1	1	1	1	0	0	0	0	3	392	6	0	1	0	4	Q36
0	7	5	1	0	0	11	3	3	1	8	2	0	0	0	1	0	0	3	1	1	0	4	0	1	6	0	0	3	0	0	1	0	0	0	0	408	1	0	0	4	Q37
1	5	5	0	0	0	2	6	3	0	11	5	0	0	1	1	0	0	3	1	1	0	2	0	0	0	0	0	0	2	0	0	0	0	0	0	3	394	0	0	0	Q38
0	0	0	0	0	0	0	1	1	0	1	1	31	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	21	2	0	1	0	0	0	0	187	3	0	Q39
0	0	0	0	0	2	3	0	0	2	0	3	5	5	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	3	224	0	Q40
1	3	2	0	0	0	7	0	1	5	10	4	0	0	0	0	0	0	1	0	0	0	1	0	0	0	3	0	0	0	0	0	0	0	0	0	2	1	0	0	182	Q41

Figure B.7 Experiment 2, Case 3

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
237	4	1	3	1	0	27	23	29	6	12	4	2	2	0	1	0	1	3	0	0	2	1	0	0	0	0	0	1	0	0	0	0	0	2	5	4	2	2	1	1	Q1
11	182	12	2	0	2	22	32	26	7	5	6	2	1	1	1	0	5	1	0	0	3	2	0	1	0	0	0	0	0	0	0	0	0	0	2	1	1	0	0	0	Q2
1	8	222	4	0	2	16	23	30	4	19	3	0	0	1	0	0	2	1	0	0	4	0	0	1	1	0	0	0	1	0	0	0	0	3	1	4	2	0	1	0	Q3
0	1	2	206	4	5	9	17	14	10	18	9	1	2	0	0	1	6	0	2	0	2	0	1	1	0	1	0	3	4	0	0	1	0	3	0	2	1	0	0	0	Q4
2	2	2	13	187	4	11	13	22	18	28	8	0	5	0	0	2	6	1	0	0	1	1	0	0	0	0	3	7	0	0	0	0	0	2	0	0	1	1	2	0	Q5
0	1	2	6	1	239	16	17	17	19	14	8	0	3	1	0	0	8	0	0	0	3	0	0	0	0	0	0	0	2	0	0	0	0	3	1	4	0	0	0	0	Q6
0	0	0	0	0	0	192	13	14	3	6	5	3	2	0	0	0	0	2	0	2	0	0	0	0	0	0	0	0	0	1	0	0	0	4	0	0	0	1	0	0	Q7
0	1	0	0	0	0	28	124	30	0	7	6	5	6	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	6	0	0	2	3	0	Q8
0	0	0	0	0	0	11	17	184	2	3	5	2	2	0	0	0	0	3	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0	0	1	0	0	Q9
0	0	0	0	3	0	5	3	3	133	29	26	0	15	0	0	0	0	0	1	0	0	0	0	0	3	1	0	0	0	0	1	1	2	0	0	0	0	1	4	1	Q10
0	0	0	0	11	0	2	9	5	35	105	40	2	12	0	0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	3	2	1	3	0	Q11
0	0	0	0	0	0	5	5	3	21	42	120	1	30	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	1	4	2	0	Q12
0	0	0	0	0	0	7	6	2	0	1	0	210	5	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	2	7	1	1	0	0	0	0	11	5	0	Q13
0	0	0	0	0	0	2	1	1	2	3	7	1	207	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	3	3	0	Q14
0	3	2	1	0	2	13	13	22	3	8	3	0	1	122	0	0	0	1	0	0	3	0	0	0	0	1	0	0	0	0	3	0	0	0	0	1	0	0	0	0	Q15
1	1	0	4	0	0	15	22	18	3	2	4	2	0	0	124	0	1	1	0	0	2	0	0	0	0	0	0	0	1	0	0	0	1	0	2	1	0	0	0	0	Q16
1	0	1	1	0	4	1	11	12	10	10	3	0	2	1	0	127	1	0	1	0	0	0	0	0	0	1	0	0	1	0	0	0	0	2	1	3	0	0	0	0	Q17
0	0	0	0	2	3	4	12	11	7	14	1	1	1	0	0	0	125	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	2	1	2	0	0	0	0	Q18
1	5	2	1	0	4	17	18	18	6	7	2	17	0	1	1	2	3	153	0	1	2	1	0	3	0	0	1	0	0	0	0	0	0	1	2	6	2	0	0	0	Q19
2	1	0	4	0	5	8	11	20	15	14	9	0	12	0	0	0	4	1	144	0	1	1	0	0	0	0	0	0	1	0	0	0	0	3	3	2	1	0	0	0	Q20
0	1	3	0	0	2	22	10	24	2	7	4	1	0	1	0	0	0	1	0	116	0	0	0	1	0	0	1	0	2	0	0	0	0	2	1	1	0	0	0	0	Q21
0	4	20	1	0	1	13	11	21	2	11	2	2	0	0	1	0	1	1	0	6	107	0	0	0	0	0	2	1	0	0	0	0	0	3	0	2	2	0	0	0	Q22
17	0	2	0	1	4	13	12	9	4	13	5	0	0	0	0	1	0	0	1	0	2	114	5	0	3	0	1	0	0	0	0	0	0	1	1	1	0	0	0	0	Q23
0	1	0	0	0	3	12	8	17	4	11	3	0	1	0	0	0	0	0	1	0	1	6	103	9	1	0	0	0	2	0	0	0	0	0	7	2	0	0	1	1	Q24
1	0	1	1	0	0	10	6	9	8	12	8	1	1	0	0	1	0	0	0	2	0	0	4	115	1	2	1	0	1	0	0	0	0	5	5	0	0	1	0	0	Q25
2	0	2	2	1	3	9	18	14	5	10	4	1	0	0	0	0	2	2	0	0	0	2	0	1	112	2	1	0	0	0	0	0	0	4	0	4	0	0	0	0	Q26
0	0	0	0	0	0	11	13	9	2	7	2	0	2	1	0	1	1	0	0	0	1	0	1	4	9	97	4	0	0	0	0	0	0	0	0	16	1	2	1	0	Q27
0	0	1	1	2	24	6	14	14	12	13	3	2	1	0	1	0	4	2	0	0	1	0	0	1	0	2	96	1	0	0	0	0	0	2	0	1	0	0	0	0	Q28
1	1	0	21	5	1	9	8	8	8	11	5	0	4	0	0	0	1	0	0	1	3	2	0	0	0	0	0	80	13	0	0	0	0	2	0	3	2	0	0	0	Q29
1	0	0	1	1	3	7	7	15	12	11	4	1	3	0	0	0	0	1	0	0	4	1	1	0	0	0	0	2	149	0	0	0	0	3	1	0	1	0	0	0	Q30
0	0	0	0	0	0	1	0	0	1	0	1	15	4	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	52	1	0	0	0	0	0	0	4	2	0	Q31
0	0	0	0	0	0	1	1	1	0	0	1	14	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	58	0	1	0	0	0	0	2	4	0	Q32
0	0	0	0	0	0	1	1	0	1	2	2	1	10	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	40	1	0	0	0	0	1	2	0	Q33
0	0	0	0	0	0	1	0	0	0	0	2	2	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	46	0	0	0	0	0	4	0	Q34
1	1	3	6	0	4	22	25	23	19	24	8	1	5	0	0	0	2	1	1	0	4	1	0	0	1	1	0	0	2	0	1	0	0	314	3	5	0	1	1	0	Q35
0	1	0	1	0	3	24	18	23	23	24	5	2	3	0	0	2	5	0	1	0	3	0	3	5	0	0	1	0	4	0	0	0	0	9	293	6	3	0	2	0	Q36
3	2	3	4	2	7	29	33	34	14	20	6	2	0	0	3	0	1	1	0	0	3	0	2	0	3	1	1	0	0	0	0	0	0	2	1	292	4	1	1	0	Q37
3	2	2	4	1	2	23	38	29	4	15	2	4	2	1	0	0	3	2	1	0	5	0	0	0	0	0	0	0	5	0	0	0	0	0	2	5	291	0	0	0	Q38
0	0	0	0	0	0	1	4	3	2	2	2	85	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	14	3	0	1	0	0	0	0	126	4	0	Q39
0	0	0	0	0	0	4	3	2	6	5	2	5	21	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	3	2	3	2	0	0	0	1	10	182	0	Q40
1	0	1	0	0	1	6	5	2	3	3	2	0	1	0	0	0	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	192	Q41

Figure B.8 Experiment 2, Case 4

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
376	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
15	298	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q2
0	5	344	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	321	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	1	0	0	0	0	0	0	Q4
0	0	0	15	303	3	1	0	1	0	9	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	1	Q5
0	0	0	0	1	359	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2	0	Q6
0	0	0	0	0	0	229	4	0	0	0	0	2	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	0	Q7
0	0	0	0	0	0	23	174	10	0	0	0	1	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	9	0	0	0	0	0	Q8
0	0	0	0	0	0	0	1	224	0	0	0	2	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	Q9
0	0	0	0	2	0	0	0	0	212	11	2	0	3	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	22	0	0	0	0	28	139	25	0	6	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	7	0	0	0	Q11
0	0	0	0	4	0	0	0	0	2	14	197	0	8	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	256	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	0	0	233	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	1	0	0	200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	187	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	1	0	3	0	0	0	22	0	0	0	0	0	251	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	2	2	0	23	0	0	0	0	0	0	235	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	198	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q21
0	3	29	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	8	172	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
22	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	183	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	2	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	9	166	10	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	Q24
1	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	191	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	6	188	5	0	0	0	0	0	0	0	0	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	15	157	1	0	0	0	0	0	0	0	11	0	0	0	1	Q27
0	0	0	0	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	177	0	0	0	0	0	0	1	0	0	0	0	0	0	Q28
0	0	0	19	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	147	17	0	0	0	0	0	0	1	0	0	0	0	Q29
0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	222	0	0	0	0	0	0	3	0	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	80	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	84	0	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	61	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	Q34
0	0	0	0	0	0	4	0	1	1	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	469	0	0	0	0	0	0	Q35
0	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	455	1	0	0	0	0	Q36
0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	469	1	0	0	1	Q37
0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	3	437	0	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	103	1	0	0	Q39
0	0	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	0	Q40
0	0	0	0	1	0	3	0	1	5	6	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	201	Q41

Figure B.9 Experiment 2, Case 5

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
375	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
16	293	11	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	2	3	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q2
0	6	346	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	319	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3	0	0	0	0	0	0	0	0	0	0	0	0	Q4
0	0	0	15	290	5	0	0	2	1	17	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	2	0	0	0	0	0	0	0	0	0	0	0	Q5
0	0	0	0	2	355	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	2	0	0	Q6
0	0	0	0	0	0	220	3	0	0	0	1	0	0	0	0	0	0	4	0	7	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	0	Q7
0	0	0	0	0	0	17	171	14	0	0	0	2	0	0	0	0	0	3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	10	5	0	0	0	0	0	0	Q8
0	0	0	0	0	0	0	1	225	0	0	0	2	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q9
0	0	0	0	2	0	0	0	0	209	11	2	0	4	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	26	0	0	0	0	23	133	27	0	9	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	6	0	0	0	0	Q11
0	0	0	0	4	0	0	0	0	6	20	180	0	8	0	0	0	0	0	7	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	10	0	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	259	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	1	0	0	0	230	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	200	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	194	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	0	0	0	0	0	0	20	0	0	0	0	0	257	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	1	1	0	23	0	0	0	0	0	0	237	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	0	187	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	Q21
1	1	35	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	4	171	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
32	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	171	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	7	164	11	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	Q24
0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	192	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	192	6	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	165	2	0	1	0	0	0	0	0	5	0	0	0	0	0	Q27
0	0	0	0	0	40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	162	0	1	0	0	0	0	0	0	0	0	0	0	0	Q28
0	0	0	28	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	148	8	0	0	0	0	0	1	0	0	0	0	0	Q29
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	216	0	0	0	0	1	0	5	0	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	72	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	81	0	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	59	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	60	0	0	0	0	0	0	0	Q34
0	0	0	0	0	16	0	1	1	0	3	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	1	0	0	0	0	0	455	0	0	0	0	0	0	Q35
0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	4	457	0	0	0	0	0	Q36
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	469	2	0	1	1	Q37
0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	1	436	0	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	204	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	26	0	0	0	0	0	0	0	25	1	0	0	0	Q39
0	0	0	0	0	2	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	0	0	Q40
0	0	0	0	0	0	2	0	0	6	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	1	0	204	0	Q41

Figure B.10 Experiment 2, Case 6

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
375	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
17	296	12	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q2
0	7	346	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	323	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	Q4
0	0	0	13	309	1	1	0	0	0	12	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	1	Q5
0	0	0	0	1	359	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	1	0	Q6
0	0	0	0	0	0	229	3	0	0	0	0	3	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0	Q7
0	0	0	0	0	0	19	180	13	0	0	0	0	0	0	0	0	0	4	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2	4	0	0	0	0	0	0	Q8
0	0	0	0	0	0	0	1	226	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q9
0	0	0	0	0	0	0	0	0	215	7	5	0	3	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	15	0	0	0	0	25	145	32	0	7	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	4	0	0	0	0	Q11
0	0	0	0	1	0	0	0	0	2	17	200	0	8	0	0	0	0	0	4	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	4	0	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	257	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	0	0	232	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	1	0	0	198	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	202	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	191	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	185	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	0	0	3	0	0	0	18	0	0	0	0	0	256	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	3	3	0	0	25	0	0	0	0	0	0	231	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	199	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	Q21
0	1	16	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	9	186	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
6	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	198	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	2	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	7	166	10	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	Q24
1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	192	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q25
0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	195	3	0	0	0	0	0	0	0	0	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	15	159	0	0	0	0	0	0	0	0	10	0	0	0	1	Q27
0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	197	0	0	0	0	0	1	0	0	0	0	0	0	Q28
0	0	0	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	165	12	0	0	0	0	0	1	0	0	0	0	Q29
0	0	0	0	2	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	220	0	0	0	0	0	0	2	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	82	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	Q34
0	0	0	0	0	0	6	0	0	0	1	2	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	468	0	0	0	0	0	1	Q35
0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	456	1	0	0	0	0	Q36
0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	469	1	0	0	1	Q37
0	0	0	0	0	0	0	0	0	1	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	442	0	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	103	1	0	0	Q39
0	0	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	0	Q40
0	0	0	0	0	0	3	0	0	4	5	5	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	203	0	Q41

Figure B.11 Experiment 3, Case 1

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
373	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
20	294	13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q2
0	6	345	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	320	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	1	0	0	0	0	0	Q4
0	0	0	13	311	2	1	0	1	0	5	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	0	0	0	0	0	0	1	Q5
0	0	0	0	2	358	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	1	0	Q6
0	0	0	0	0	0	228	3	0	0	0	0	3	0	0	0	0	0	3	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	0	Q7
0	0	0	0	0	0	22	170	13	0	0	0	1	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	10	0	0	0	0	0	Q8
0	0	0	0	0	0	0	0	226	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q9
0	0	0	0	0	0	0	0	0	215	6	3	0	5	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	Q10
0	0	0	0	20	0	0	0	0	25	141	28	0	8	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	5	0	0	0	Q11
0	0	0	0	0	0	0	0	0	1	19	200	0	8	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	3	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	258	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	0	0	232	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	1	0	0	198	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	187	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	2	0	4	0	0	0	17	0	0	0	0	0	254	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	3	4	1	0	20	0	0	0	0	0	234	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	199	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q21
0	0	19	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	8	184	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
8	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	198	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	2	1	0	1	0	0	0	0	0	0	0	0	0	0	0	8	169	10	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	Q24
0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	192	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	8	188	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13	163	0	0	0	0	0	0	0	0	0	8	0	0	0	1	Q27
0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	195	0	0	0	0	0	0	0	1	0	0	0	0	0	Q28
0	0	0	16	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	155	15	0	0	0	0	0	0	1	0	0	0	0	Q29
0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5	218	0	0	0	0	0	0	0	3	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	85	0	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	Q34
0	0	0	0	0	0	3	0	1	1	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	470	0	0	0	0	0	0	Q35
0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	456	1	0	0	0	0	Q36
0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	470	1	0	0	1	Q37
0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	441	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	103	1	0	Q39
0	0	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	Q40
0	0	0	0	1	0	3	0	1	5	6	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	201	Q41

Figure B.12 Experiment 3, Case 2

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
372	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
20	292	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q2
0	5	346	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	321	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	Q4
0	0	0	13	303	3	1	0	1	0	9	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	0	0	0	1	Q5
0	0	0	0	1	359	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2	0	Q6
0	1	0	0	0	0	229	0	0	0	0	0	2	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	Q7
0	0	0	0	0	0	20	176	11	0	0	0	1	0	0	0	0	0	3	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3	8	0	0	0	0	0	Q8
0	0	0	0	0	0	0	0	224	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	Q9
0	0	0	0	0	0	0	0	0	213	7	3	0	7	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	18	0	0	0	0	23	149	25	0	6	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	6	0	0	0	Q11
0	0	0	0	0	0	0	0	0	1	11	208	0	7	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	3	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	258	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	0	0	0	0	232	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	0	0	0	1	0	0	199	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	4	0	4	0	0	0	16	0	0	0	0	0	253	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	3	4	0	0	22	0	0	0	0	0	233	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	198	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	Q21
0	1	22	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	8	180	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
7	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	198	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	2	1	0	1	0	0	0	0	0	0	0	0	0	0	0	8	167	9	0	0	0	0	0	0	0	0	0	0	6	0	0	0	0	0	Q24
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	189	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	3	192	4	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	15	157	1	0	0	0	0	0	0	0	0	11	0	0	0	1	Q27
0	0	0	0	0	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	191	0	0	0	0	0	0	0	1	0	0	0	0	0	Q28
0	0	0	15	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	157	14	0	0	0	0	0	0	1	0	0	0	0	Q29
0	0	0	0	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	220	0	0	0	0	0	0	0	2	0	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	0	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	85	0	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	64	0	0	0	0	0	0	0	Q34
0	0	0	0	0	0	5	0	1	1	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	468	0	0	0	0	0	0	Q35
0	1	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	455	1	0	0	0	0	Q36
0	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	469	1	0	0	1	Q37
0	0	0	0	0	0	0	0	0	0	1	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	2	439	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	103	1	0	Q39
0	0	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	Q40
0	0	0	0	1	0	3	0	0	7	4	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	203	Q41

Figure B.13 Experiment 3, Case 4

Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30	Q31	Q32	Q33	Q34	Q35	Q36	Q37	Q38	Q39	Q40	Q41	
371	2	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q1
21	294	12	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q2
0	5	346	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q3
0	0	0	321	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	Q4
0	0	0	10	302	4	0	0	1	0	13	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	1	0	0	0	0	0	0	Q5
0	0	0	0	1	358	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	2	0	Q6
0	0	0	0	0	0	225	4	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	12	0	0	0	0	0	0	Q7
0	2	0	0	0	0	14	180	11	0	0	0	1	0	0	0	0	0	3	0	0	0	0	2	0	0	0	0	0	0	0	0	0	4	6	0	0	0	0	0	Q8
0	0	0	0	0	0	0	1	225	0	0	0	3	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	Q9
0	0	0	0	0	0	0	0	0	213	8	5	0	3	0	0	0	0	0	2	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q10
0	0	0	0	19	0	0	0	0	23	147	24	0	7	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	5	0	0	0	0	Q11
0	0	0	0	2	0	0	0	0	2	17	200	0	7	0	0	0	0	0	3	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	4	0	0	0	0	Q12
0	0	0	0	0	0	0	0	0	0	0	0	258	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q13
0	0	0	0	0	0	0	0	0	1	0	2	0	229	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q14
0	0	0	0	0	0	0	0	1	0	0	0	0	0	198	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	Q15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	204	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	Q16
0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	193	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	188	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q18
0	0	0	0	0	0	2	0	1	0	0	0	17	0	0	0	0	0	257	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q19
0	0	0	0	0	0	0	0	0	2	5	1	0	20	0	0	0	0	0	234	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q20
0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	199	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q21
0	2	26	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	5	177	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q22
5	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	200	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q23
0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	9	168	9	0	0	0	0	0	0	0	0	6	0	0	0	0	0	Q24
0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	190	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Q25
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	8	183	7	0	0	0	0	0	0	1	1	0	0	0	0	Q26
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	19	159	0	0	0	0	0	0	0	1	6	0	0	0	Q27
0	0	0	1	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	189	0	0	0	0	0	0	0	0	0	0	0	Q28
0	0	0	19	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	155	13	0	0	0	0	0	1	0	0	0	0	Q29
0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	221	0	0	0	1	1	1	0	2	0	0	Q30
0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	80	0	0	0	0	0	0	0	0	0	Q31
0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	85	0	0	0	0	0	0	0	0	Q32
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	0	Q33
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	63	0	0	0	0	0	0	Q34
0	0	0	0	0	0	8	0	0	0	3	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	466	0	0	0	0	0	Q35
0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	4	455	0	0	0	0	Q36
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	469	2	0	0	2	Q37
0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	441	0	0	0	Q38
0	0	0	0	0	0	0	0	0	0	0	0	153	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	102	1	0	Q39
0	0	0	0	0	2	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	248	0	Q40
0	0	0	0	0	0	0	0	0	4	7	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	208	Q41

Figure B.14 Experiment 3, Case 5