

**ANOMALY MODELLING AND DETECTION FOR SMART  
GRID COMMUNICATION INFRASTRUCTURES**

BY

SAIF AHMAD

A Thesis Presented to the  
DEANSHIP OF GRADUATE STUDIES

**KING FAHD UNIVERSITY OF PETROLEUM & MINERALS**

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the  
Requirements for the Degree of

**MASTER OF SCIENCE**

In

**COMPUTER NETWORKS**

JANUARY 2013

ANOMALY MODELING AND DETECTION  
FOR SMART GRID COMMUNICATION  
INFRASTRUCTURES

by

**SAIF AHMAD**

A Thesis Presented to the  
DEANSHIP OF GRADUATE STUDIES

In Partial Fulfillment of the Requirements  
for the degree

**MASTER OF SCIENCE**

**IN**

**COMPUTER NETWORKS**

KING FAHD UNIVERSITY  
OF PETROLEUM & MINERALS

Dhahran, Saudi Arabia

JANUARY 2013


KING FAHD UNIVERSITY OF PETROLEUM & MINERALS  
DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

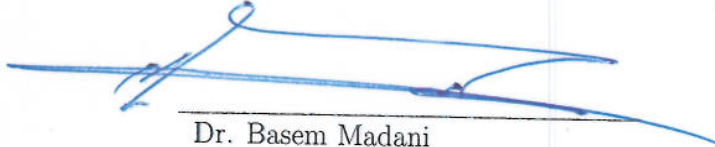
This thesis, written by **SAIF AHMAD** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER NETWORKS**.

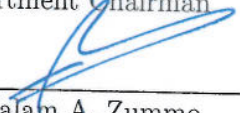
Thesis Committee

  
\_\_\_\_\_  
Dr. Zubair Ahmed Baig (Adviser)

  
\_\_\_\_\_  
Dr. Sadiq M. Sait (Member)

  
\_\_\_\_\_  
Dr. Ahmad Almulhem (Member)

  
\_\_\_\_\_  
Dr. Basem Madani  
Department Chairman

  
\_\_\_\_\_  
Dr. Salam A. Zummo  
Dean of Graduate Studies

12/1/13  
\_\_\_\_\_  
Date



©Saif Ahmad  
2013

*Dedication*

*For my family, who offered me unconditional love and support  
throughout the course of this thesis.*

# ACKNOWLEDGMENTS

*All the praise is for Allah, the most merciful and beneficent, who blessed me with the knowledge, gave me the courage and allowed me to accomplish this work.*

*At the end of my thesis I would like to thank all those people who made this thesis possible. First of all, I want to express my sincere appreciation to my advisor Dr. Zubair Baig who offered his continuous advice and encouragement throughout the course of this thesis. I thank him for the guidance and great effort he put into training me in the scientific field. Besides my advisor, I would like to thank the rest of my thesis committee: Dr. Sadiq M. Sait and Dr. Ahmad Almulhem, for their encouragement, remarkable suggestions, constructive criticism and friendly discussion provided by all.*

*I am indebted to the Computer Engineering Department at KFUPM and the instructors there for instilling relevant knowledge into me. In addition to the instructors at KFUPM, I was fortunate enough to have the company of many good friends. In particular, I cannot thank Saad Khan enough for his exceptional friendship and timely feedback*

*Finally, I take this opportunity to express the profound gratitude to my beloved parents and my brothers for their love and continuous support.*



# TABLE OF CONTENTS

<b>LIST OF TABLES</b>	<b>ix</b>
<b>LIST OF FIGURES</b>	<b>x</b>
<b>ABSTRACT (ENGLISH)</b>	<b>xi</b>
<b>ABSTRACT (ARABIC)</b>	<b>xii</b>
<b>CHAPTER 1 INTRODUCTION</b>	<b>1</b>
1.1 Traditional Grid . . . . .	1
1.2 Smart Grid (SG) . . . . .	2
1.3 Smart Grid expectations . . . . .	4
1.3.1 Support for Various Devices . . . . .	4
1.3.2 Superior Power Quality . . . . .	4
1.3.3 Operation Efficiency and Optimization . . . . .	5
1.3.4 Grid Security . . . . .	5
1.3.5 Grid Self-Correction . . . . .	6
1.3.6 Consumer Participation . . . . .	6
1.3.7 Market Boost . . . . .	6
1.4 Smart Grid Domains . . . . .	7
1.4.1 Bulk Generation . . . . .	7
1.4.2 Transmission . . . . .	8
1.4.3 Distribution . . . . .	9
1.4.4 Customer . . . . .	9



1.4.5	Operations . . . . .	10
1.4.6	Markets . . . . .	11
1.4.7	Service Provider . . . . .	12
1.5	Smart Grid Communications Architecture . . . . .	13
1.5.1	Home Area Networks (HAN) . . . . .	13
1.5.2	Neighborhood Area Network (NAN) . . . . .	13
1.5.3	Wide Area Network (WAN) . . . . .	14
1.5.4	Supporting Network Technologies for Smart Grid . . . . .	15
1.6	Motivation and Objective . . . . .	17
1.7	Research Contribution . . . . .	19
1.8	Thesis Outline . . . . .	20
<b>CHAPTER 2 LITERATURE REVIEW</b>		<b>22</b>
2.1	Network Security . . . . .	23
2.1.1	Types of Network Attacks . . . . .	24
2.2	Intrusion Detection . . . . .	26
2.2.1	Statistical Models . . . . .	28
2.2.2	Machine Learning Techniques . . . . .	30
2.3	Security Implications of Smart Grid . . . . .	42
2.4	Vulnerable Smart Grid Domains . . . . .	44
2.4.1	PCS Security . . . . .	44
2.4.2	Smart Meter Security . . . . .	45
2.4.3	Power System State Estimation Security . . . . .	48
2.4.4	Smart Grid Communication Protocol Security . . . . .	49
<b>CHAPTER 3 FUZZY-BASED OPTIMIZATION FOR EFFEC-</b>		
<b>TIVE DETECTION OF SMART GRID CYBER-ATTACKS</b>		<b>51</b>
3.1	Device Implant Attack . . . . .	53
3.2	Attack Detection Scheme . . . . .	54
3.2.1	Steps for Attack Detection . . . . .	54
3.2.2	Optimal Parameter Selection . . . . .	58

3.2.3	Multi-Objective Approach to Attack Detection . . . . .	61
3.2.4	Werners Operator . . . . .	61
3.3	Fuzzy Logic . . . . .	63
3.4	Results and Analysis . . . . .	65
3.4.1	Simulation parameters . . . . .	65
3.4.2	Simulation Results . . . . .	65
<b>CHAPTER 4 SMART GRID DEVICE BEHAVIOR DATASET</b>		<b>71</b>
4.1	Dataset Generation . . . . .	72
4.2	UMass Smart* dataset . . . . .	77
<b>CHAPTER 5 SUPPORT VECTOR MACHINE (SVM) BASED SG INTRUSION DETECTION</b>		<b>79</b>
5.1	Support Vector Machine (SVM) . . . . .	80
5.1.1	Two-Class Classification . . . . .	80
5.1.2	Multi-Class Classification . . . . .	83
5.2	Results and Analysis . . . . .	83
5.2.1	Weka Tool . . . . .	84
5.2.2	Training . . . . .	84
5.2.3	Testing . . . . .	84
<b>CHAPTER 6 SELF-ORGANIZING MAP (SOM) BASED AT- TACK DETECTION FOR SMART GRID</b>		<b>87</b>
6.1	Self-Organizing Maps (SOMs) . . . . .	88
6.1.1	The SOM Structure . . . . .	88
6.1.2	Preprocessing . . . . .	89
6.1.3	SOM Training . . . . .	90
6.1.4	SOM Testing . . . . .	93
6.2	Simulation Results . . . . .	93
6.2.1	True Positives versus False Positives (Fixed Attack to Nor- mal Ratio) . . . . .	94

6.2.2 Execution Time . . . . .	98
<b>REFERENCES</b>	<b>99</b>
<b>VITAE</b>	<b>110</b>

# LIST OF TABLES

1.1	Traditional Grid Vs Smart Grid [1]. . . . .	3
3.1	Simulation Parameters. . . . .	65
3.2	Simulation Results for $N = 20$ and $\gamma = 0.25$ . . . . .	66
3.3	Simulation Results for $N = 20$ and $\gamma = 0.5$ . . . . .	67
3.4	Simulation Results for $N = 20$ and $\gamma = 0.75$ . . . . .	68
3.5	Simulation Results for $N = 20$ and $\gamma = 1$ . . . . .	69
4.1	Power Ratings for Common Household Devices. . . . .	72
4.2	Energy Consumption (kWh) of Home Appliances. . . . .	73
4.3	Basic Dataset Characteristics. . . . .	75
4.4	Sample Dataset Rows. . . . .	76
4.5	Basic Smart* Dataset Characteristics. . . . .	78
5.1	SVM Testing Results. . . . .	85
5.2	SVM Confusion Matrix. . . . .	85
6.1	SOM Training Parameters. . . . .	94

# LIST OF FIGURES

1.1	Traditional power grid infrastructure. . . . .	2
1.2	Bulk Generation domain. . . . .	7
1.3	Distribution domain. . . . .	9
1.4	Customer domain. . . . .	10
1.5	Operations domain. . . . .	11
1.6	Markets domain. . . . .	12
1.7	Service Provider domain. . . . .	12
3.1	The proposed device implant attack detection scheme. . . . .	55
3.2	Smart devices communicate at regular intervals. . . . .	55
3.3	The proposed attack detection scheme. . . . .	58
5.1	Optimal hyperplane for a two-class input space. . . . .	81
6.1	Typical SOM Architecture. . . . .	89
6.2	TP VS FP with 25% ratio dataset. . . . .	95
6.3	TP VS FP with 35% ratio dataset. . . . .	96
6.4	TP VS FP with 45% ratio dataset. . . . .	96
6.5	TP VS FP with 55% ratio dataset. . . . .	96
6.6	TP VS FP with 65% ratio dataset. . . . .	97
6.7	TP VS FP with 50% ratio dataset. . . . .	97
6.8	Execution time of SOM training for varying map sizes. . . . .	98

# THESIS ABSTRACT

**NAME:** Saif Ahmad

**TITLE OF STUDY:** Anomaly Modeling and Detection for Smart Grid  
Communication Infrastructures

**MAJOR FIELD:** Computer Networks

**DATE OF DEGREE:** January 2013

*The current power grid is outdated and overwhelmed by the increase in demand for power. The advent of the smart grid presents a new paradigm that will solve this problem and also provide several unique functionalities to the consumers. The smart grid is envisioned to be a completely automated infrastructure that will require little or no human intervention. This will be made possible due to the integration of latest information and communications technologies (ICT) into the power grid. The various sensors installed in the smart grid will have the capability to report back information related to power consumption, billing and other significant readings. However, this integration of technology also raises several concerns about the cyber protection of the smart grid. The security challenges presented by the smart grid are unique and cannot be overcome with existing solutions. This work presents a novel intrusion detection technique for the smart grid infrastructure that is capable of detecting malicious activity at different levels of the smart grid hierarchy. In addition signatures of anomalous smart grid behaviors are formulated to improve detection rate.*

## ملخص الرسالة

الاسم الكامل: سيف أحمد

عنوان الرسالة: " نمذجة وكشف الشذوذ للبنية التحتية للاتصالات الشبكة الذكية "

التخصص: " شبكات الحاسب "

تاريخ الدرجة العلمية: يناير ٢٠١٣

أصبحت شبكة الطاقة الحالية قديمة وتضغى عليها بالزيادة في طلب الطاقة. فإن حلول الشبكة الذكية تقدم نموذجاً جديداً سيحل هذه المشكلة وستوفر وظائف فريدة من نوعها للمستهلكين. ومن المتوقع ان تكون الشبكة الذكية ببنية تحتية آلية بالكامل تتطلب قليل او معدومة من التدخل البشري. هذا سوف يتم بطريقة ممكنة لإندماج آخر تكنولوجيا المعلومات والاتصالات (ICT) في شبكة الطاقة. أجهزة الاستشعار المختلفة المثبة في الشبكة الذكية لديها القدرة لتقديم تقرير عن المعلومات المتعلقة باستهلاك الطاقة والفواتير وغيرها من القراءات الهامة. ومع ذلك فإن هذا الاندماج للتكنولوجيا يثير أيضاً العديد من المخاوف المتعلقة بحماية الانترنت للشبكة الذكية. فان التحديات الامنية المتقدمة من الشبكة الذكية تكون فريدة من نوعها ولا يمكن التغلب عليها بالحلول الموجودة. هذا العمل يقدم تفاصيل كشف التسلسل التقني للبنية التحتية للشبكة الذكية القادرة علي كشف النشاط الضار علي مستويات مختلفة من التسلسل الهرمي للشبكة الذكية. في التوقعات الاضافية لسلوكيات الشبكة الذكية الشاذة تصاغ لتحسين معدل الكشف.

# CHAPTER 1

## INTRODUCTION

### 1.1 Traditional Grid

The main objective of the traditional power grid is to transfer electricity from the producers (coal plants, hydroelectric dams, etc.) to the consumers (households and businesses). It is a centralized model where fixed generation plants supply consumers through timeworn, unidirectional communication and circulation systems. Figure 1.1 [2] shows the traditional power grid. The high-voltage wires and substations that transport electricity over large distances constitute the transmission system. The distribution structure consists of moderate-voltage wires and substations that move power in the nearby locations. For long haul transmissions to substations, step-up transformers are used to enhance the voltage. In addition the voltage is curtailed when transferring over medium voltage power lines to the consumer locations. This is realized by applying pole-top transformers. The traditional grid has failed to cope up with the advances in technology over the years



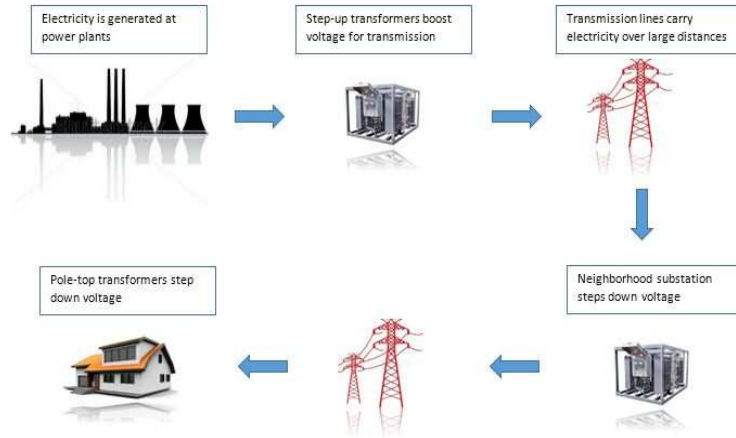


Figure 1.1: Traditional power grid infrastructure.

whereas the demand for power has increased rapidly. The present-day grid without communication is simply a broadcaster of power without any concern about the power requirement at the consumer end. Therefore, it is imperative that a two-way communication channel is set-up between the producer and the consumer to ensure that only the required amount of power is delivered to the consumers. Communication enables utilities to achieve three key objectives: intelligent monitoring, security, and load balancing [3].

## 1.2 Smart Grid (SG)

The smart grid is a contemporary electric power grid setup that provides improved efficiency, reliability and safety, with smooth integration of renewable and alternative energy sources, through automated control and modern communications technologies [4]. This progressive arrangement provides end users with real-time monitoring and controlling capabilities of energy consumption across the smart

communication network. Table 1.1 [1] gives a brief comparison between the traditional grid and the smart grid features.

<b>Traditional Grid</b>	<b>Smart Grid</b>
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors throughout
Manual monitoring	Self-monitoring
Manual restoration	Self-healing
Failures and blackouts	Adaptive and islanding
Limited control	Pervasive control
Few customer choices	Many customer choices

Table 1.1: Traditional Grid Vs Smart Grid [1].

The combination of contemporary information and communication technologies, enables the SG to handle a range of situations and events. This implies that the SG could respond to events that occur anywhere in the grid, such as power generation, transmission, distribution, and consumption, and adopt the corresponding response strategies. For example, on detection of a medium voltage transformer failure in the distribution grid, the SG may automatically adjust the flow of electricity and recover the power delivery service [1]. In addition, the SG empowers the consumers to outsource the excess energy that is generated and stored by them.

## **1.3 Smart Grid expectations**

The smart grid is expected to bring with it a number of new technological advances in addition to addressing the existent issues of the traditional grid. This section presents some of the outcomes expected from the introduction of the smart grid and its implications [5].

### **1.3.1 Support for Various Devices**

The smart grid is projected to support a variety of storage and power generation devices and also enable two-way energy exchange on the present grid. This implies that in addition to supporting distributed energy resources (DERs) like wind energy, storage batteries and photovoltaic cells, the smart grid will also facilitate traditional electric loads, smart devices in households and plug-in electric vehicles (PEVs). The use of distributed energy resources allows users to gain financial benefits because they have the choice to retail the surplus energy back to the grid. The two-way energy exchange mechanism will also alleviate the problem of energy scarcity at the customer or utility end.

### **1.3.2 Superior Power Quality**

The ability of the supplied electricity on the distribution grid to stick-to the specified peak levels or root mean square (RMS) voltages is defined as power quality. The loads involved in the grid are intended to work at definite levels of electric voltage and frequency and hence cannot tolerate any fluctuation of voltage

level. On the other hand the affected load can harm the grid affecting customers residing on the same site. This can even lead to power outages causing revenue losses. The smart grid overcomes such issues by enhancing the power quality through monitoring and conditioning. Since electrical devices in the modern world need significantly higher power quality, a smart grid is able to regulate the power quality while still maintaining load sensitivity. This provides flexibility in terms of pricing.

### **1.3.3 Operation Efficiency and Optimization**

The use of computer technology for widespread facility and electrical field equipment checking will enable the smart grid to minimize losses and also to operate the grid more effectively. The gathered information will ease the maintenance cycle and will also help in improving the electrical power systems design process.

### **1.3.4 Grid Security**

Since the smart grid will be heavily dependent on the use of an integral communications network for many of its functions such as control and monitoring, the protection of the infrastructure against cyber or physical attacks is extremely important. The smart grid must be able to detect as well as segregate any similar malicious attempts.

### **1.3.5 Grid Self-Correction**

The smart grid is estimated to be highly fault tolerant and thus it will be capable of taking appropriate actions in a timely manner in case of fault detection without the need for any human involvement. This would make the smart grid highly reliable, maximize its power quality and productivity and minimize service outage time.

### **1.3.6 Consumer Participation**

The smart grid will enable a greater participation of the consumers due to its flexible pricing schemes with rates varying according to the load on the grid and programs like demand response that allow for temporary reduction of load on the grid. The communications intelligence integrated into the smart grid gives the end users the option to monitor the health of their individual smart appliances and supplant the inefficient ones.

### **1.3.7 Market Boost**

The SG will act as a hub for a large number of new consumer services including the ability to retail and obtain electricity from diverse traders. This will in turn make the market much more competitive with a large number of electricity suppliers involved and a variety of options available to the consumers. In addition, the market vendors will be able to take advantage of variable pricing to manage the demand of electricity with its availability. The market vendors will need to employ open standards of communication to ease the process of billing of user data.

## 1.4 Smart Grid Domains

The major domains of a smart grid defined by the National Institute of Standards and Technology (NIST) include Bulk Generation, Transmission, Distribution, Customers, Operations, Markets and Service Providers [6, 7].

### 1.4.1 Bulk Generation

The Bulk Generation domain is responsible for generating electricity in large amounts using renewable and non-renewable energy sources. The renewable sources can either be either variable sources (e.g., solar and wind) or non-variable sources (e.g., hydro, biomass, geothermal and pump storage). The non-renewable sources include nuclear, coal and gas. The resources used by the Bulk Generation domain are highlighted in Figure 1.2.

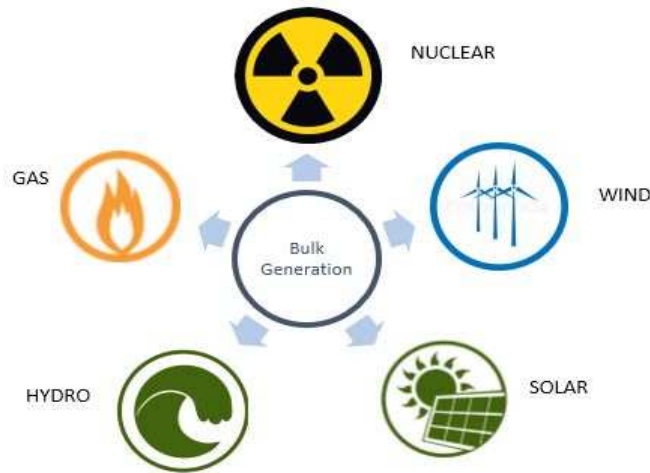


Figure 1.2: Bulk Generation domain.

This domain also stores energy for later distribution. The Bulk Generation do-

main is the most critical component of the smart grid as it is connected to the Transmission domain and without transmission it would not be possible to serve the customers [7]. This domain also maintains key performance and quality of service parameters such as shortage of supply (especially for variable sources) and generator failure which can be used to route electricity to the Transmission domain from other sources.

### **1.4.2 Transmission**

The Transmission domain is used to transport electricity over long distances from from generation sources to distribution through several substations. The main responsibility of this domain is to maintain consistency on the electric grid by balancing between generation (supply) with load (demand) across the transmission network. A transmission network is generally under the control of a Regional Transmission Operator or Independent System Operator (RTO/ISO) [7].

### 1.4.3 Distribution

The Distribution domain (see Figure 1.3) handles allocation of the electricity sent and received by the end customers in the smart grid. This domain links all intelligent field devices and the Smart Meters available in the grid.

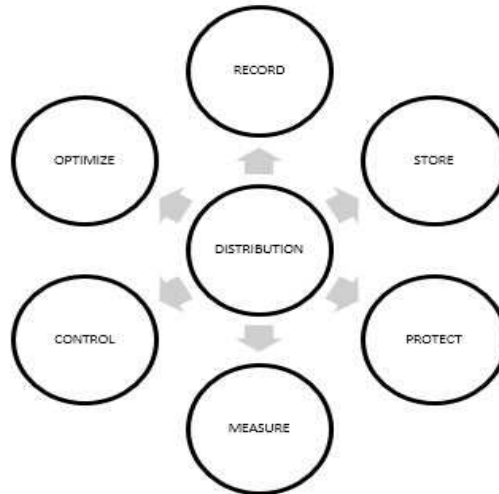


Figure 1.3: Distribution domain.

The distribution domain also manages and controls these devices via a bidirectional wireless or wired communications network. It is also possible that the distribution network may be attached to other energy storage services at the distribution level.

### 1.4.4 Customer

The Customer domain of the Smart Grid is responsible for connecting the end-users of electricity to the electric distribution network through Smart Meters. The smart meters handle the flow of electricity by the customer and provide usage



statistics. Each customer is in charge of a unique area comprised of electricity premise and bidirectional communications networks. Major functions handled by this domain are summarized in Figure 1.4.

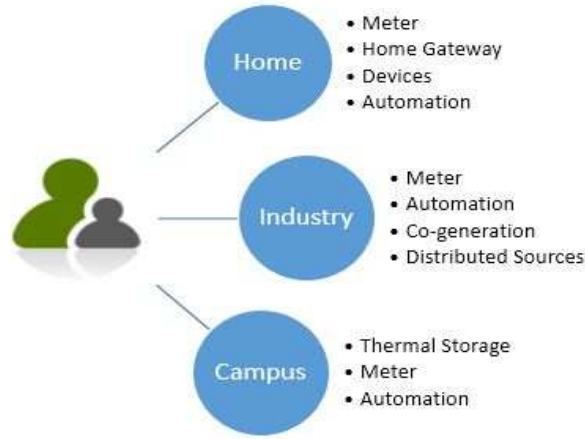


Figure 1.4: Customer domain.

This domain may also generate, store and manage the use of energy, as well as the connectivity with plug-in vehicles (PEVs).

### 1.4.5 Operations

The Operations domain (see Figure 1.5) executes and restricts the flow of electricity from all other domains in the Smart Grid. It performs supervisory tasks such as monitoring, reporting, controlling and processing of relevant information. It also establishes a two-way communication channel that links it to substations, customer premises networks and other intelligent field devices.

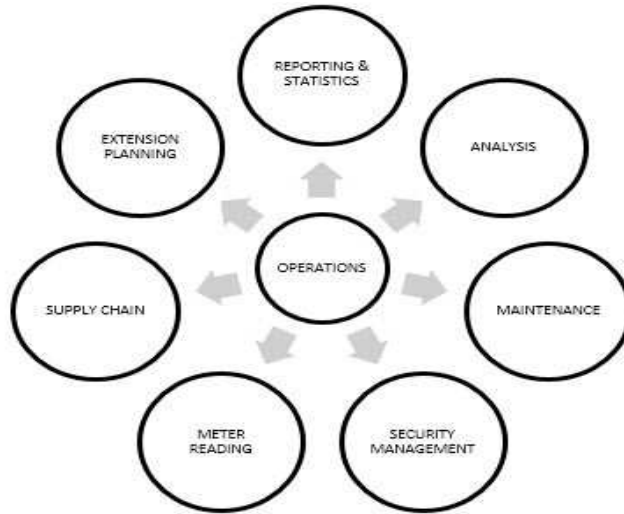


Figure 1.5: Operations domain.

Business intelligent mechanisms are integrated in this domain to make the decision making task more accurate. Examples of typical actions performed by the Operations domain may include: network operation and maintenance, usable reporting and statistics, fault management, security management and others.

#### 1.4.6 Markets

The task of coordinating and operating all involved parties in Smart Grid is done by the markets domain. It offers the market organization, wholesaling, retailing and trading of energy services. It also handles information exchange with third-parties. Major functions performed by this domain are summarized in Figure 1.6.



Figure 1.6: Markets domain.

### 1.4.7 Service Provider

The Service Provider domain is responsible for all third-party related processes such as energy management related information which are shown in Figure 1.7. Additional tasks that may be handled by the domain include demand response programs, outage management and field services.

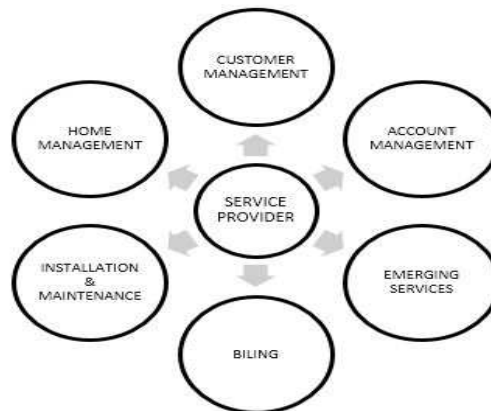


Figure 1.7: Service Provider domain.

## **1.5 Smart Grid Communications Architecture**

The Smart Grid infrastructure is known to consist of three network layers: home area networks (HAN), neighborhood area networks (NAN), and wide area networks (WAN) [8]. Each of these layers is composed of several modules or controlling systems which may be expanded in the future to incorporate new modules and systems.

### **1.5.1 Home Area Networks (HAN)**

The HAN is responsible for establishing communication among devices in the home whereas the HAN gateway communicates with the neighborhood-area network [8]. It provides monitoring and control facilities at customer homes and implements advanced functionalities like Demand Response (DR) and Automatic Metering Infrastructure (AMI). The HAN is comprised of the service module (SM), the metering module (MM), and the meter controlling system (MCS). The SM is responsible for providing real-time information related to energy consumption and price to the end-users whereas information about energy consumption in a consumers home is stored by the MM. The MCS accumulates and controls the information transmitted from SM and MM.

### **1.5.2 Neighborhood Area Network (NAN)**

NAN forms the second layer of the Smart Grid communications infrastructure and consists of multiple interconnected MCSs of HAN that are in close vicinity

to each other [8]. In addition to these the NAN also contains: the central access controller (CAC) and the smart meter data collector (SMDC). The CAC behaves as the interface that manages the communication between the energy supplier and HANs. The SMDC handles the metering records of the whole community. One of the main requirements of NAN is to support mesh networking, as the network needs to cover thousands of homes, essentially covering over a few square miles. These networks also have to provide low latencies, typically less than 10 seconds as control signals are part of the two way communication.

### **1.5.3 Wide Area Network (WAN)**

The WAN constitutes the final layer of the Smart Grid infrastructure and is responsible for providing communication between the highly scattered smaller area networks that serve the power systems at different locations [8]. The components of this layer include the energy distribution system (EDS), the supervisory control and data acquisition (SCADA) controller, and the energy and service corporations (E&SC). The EDS handles the distribution of energy and metering data. The SCADA controller manages the grid elements distribution. The metering and control information accumulated is then transmitted to the E&SC which makes advanced decisions on price.

### 1.5.4 Supporting Network Technologies for Smart Grid

There are a number of available communication technologies that can be used in the different components of the Smart Grid. However, there is no single technology that meets the requirements of all the applications. The following are some of these technologies:

- *Powerline Communication (PLC)*: Powerline Communication (PLC) lends its support to the Smart Grid due to its ability to transmit high-speed data signals between different devices over the existing power lines [9]. In a typical PLC network, powerlines are used to link Smart Meters to the data concentrator through powerlines and cellular network technologies provide the medium through which data is transferred to the data center. PLCs provide good coverage but at the cost of poor bandwidth and latency. Therefore, PLCs are mostly suitable for in-door environment.
- *HomePlug*: Another efficient strategy that takes advantage of the existent electricity infrastructure for communication is called HomePlug [10]. A user may create a network by either connecting two or more adapters to the power outlets in the home or the devices may have built-in HomePlug adapter capabilities. Several versions of HomePlug exist like HomePlug 1.0 which supports speeds up to 14 Mbps and HomePlug AV that supports speeds up to 200 Mbps.
- *M-Bus*: M-Bus (Meter-Bus) [10] is a European standard that allows for remote reading of different types of consumption meters like gas or electricity

meters. The M-Bus interface is highly cost effective as it supports communication on two wires. The primary purpose of M-Bus is to facilitate for the networking and remote reading of utility meters. An application of M-Bus is the measurement of gas or water consumed by an end user.

- *ZigBee*: The Zigbee [10] protocol is the preferred communication standard in the HAN due to its simplicity, mobility, robustness, low bandwidth requirements, low cost of deployment, its operation within an unlicensed spectrum and easy network implementation. It supports three types of bands: 868-868.6 MHz with 1 channel for European utilities, 902-928 MHz with 10 channels for North American utilities, and 2.4 GHz with 16 non-overlapping channels for worldwide utilities. ZigBee enabled Smart Meters can communicate and control the ZigBee integrated devices. The ZigBee Smart Energy Profile (SEP) allows user to get real-time information about their energy consumption. There are several factors that have hindered the widespread implementation of the Zigbee protocol. These include low processing abilities, limited memory size, strict delay requirements and potential interference with other devices, etc.
- *Z-Wave*: An alternative communication standard to Zigbee is Z-Wave [10]. Z-Wave is a closed standard available only to Zensys customers and uses the unlicensed 900 MHz ISM (Industry, Scientific and Medical) band. It supports binary mode operations and can incorporate device related information in the communications. On-off states for appliances and raise-lower

states for thermostat or volume control are examples of supported binary operations. Z-Wave is known to show good performance even in the presence of interference from common wireless devices.

The Smart Grid is envisioned to be a completely automated and intelligent setup that will offer numerous advantages over the existing power grid. The backbone of such an intelligent system is going to be a fast, reliable and secure communication network that interconnects a huge variety of devices distributed throughout its various domains. The communication architecture developed for the Smart Grid has to take into account the resource constrained nature of the Smart Grid devices and the distributed yet integrated nature of its domains.

## 1.6 Motivation and Objective

The introduction of information and communications technology into the existent electricity network promises high-end features for the end users in the form of Smart Grid. Although, the ability of the Smart Grid to cut down on the electricity utility bill for end-users, is highly praised, it also provides a platform for the launch of a multitude of malicious attacks through malicious utilization of this very communication infrastructure. Some of the potential risks faced by the Smart Grid include [11]:

- Due to greater complexity there is increased risk of accidental errors and adverse types of attacks.



- The Smart Grid incorporates a large number of interconnections between its components which makes the system highly vulnerable to attacks.
- The increasing number of smart nodes exposes a higher number of access points to the network for launching Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks.
- A large number of available network links also increases the risk of cascading failures. A cascading failure occurs when the failure of a single component (e.g., transmission line failure) triggers the failure of several other components and finally the blackout of the grid itself.

However, considering the newness of the technology, vulnerabilities of the Smart Grid infrastructure (SGI) have not been fully identified. As a result, there is a lack of quantifiable evidence to clearly identify malicious activity within the Smart Grid communications, as opposed to routine activity. Due to the nature of the SGI, contemporary security solutions may not be directly implementable for protecting the grid from the ever-present threat of malicious attacks.

This work presents a novel intrusion detection technique for the Smart Grid infrastructure that is capable of detecting malicious activity at different levels of the Smart Grid hierarchy. In addition signatures of anomalous Smart Grid behaviors are formulated to improve detection rate.

## 1.7 Research Contribution

The main contributions of this thesis are:

- *Attack Pattern Modeling:* One attack category that may be identified for the SGI is the device implant attack, wherein rogue devices may be installed within a consumers premises so as to report falsified readings to the Smart Meter. We propose a detection technique through sharing of device reading information and pattern reconstruction for eventual delivery to the Smart Meter in a timely manner. We define an optimization criteria to balance a tradeoff between high frequency of inter-device communication (high overhead) and accuracy in attack detection. To achieve this multi-objective optimization between the two parameters we employ fuzzy based optimization technique.
- *Dataset Modeling for Smart Grid:* Research within the field of Smart Grid is often constrained by the lack of accurate and standard data about current system deployments. In this direction, we propose a realistic testbed to provide a platform where we test our different detection methodologies. We model the attacks against the home area network of the SGI, through definition and generation of routine device behaviors. Any observed deviation from the defined normal profile is labeled as a malicious attack.
- *Detection of Attacks at HAN Using SVM:* We apply the support vector machine (SVM) approach to create a classification of the SGI data that allows

to distinguish normal traces from attack traces. SVMs are known to produce very accurate classifiers and are less prone to the overfitting problem.

- *Detection of Attacks at HAN Using SOM:* We propose the use of Self Organizing Maps (SOM), for data clustering, for facilitating classification of SGI data into either the normal class or the anomalous class. The proposed approach is subsequently tested for specific parameters and varying training map sizes.

## 1.8 Thesis Outline

In Chapter 2, we outline the various threats that the Smart Grid faces and survey several approaches available in literature for handling these threats. We also list several machine learning techniques that have the potential to provide novel solutions for securing the Smart Grid.

In Chapter 3, we present the formulation of the device implant attack in terms of frequency of inter-device communication and accuracy in attack detection. A fuzzy-based optimization approach is proposed towards achieving a realistic trade-off between two parameters: attack detection rate and cost of inter-device communication. The optimization is expected to provide ideal values for the parameters that will enable detection of attacks with minimum system overhead. Finally, the value of the cost ratio is varied to examine its impact on the detection scheme.

In Chapter 4, we model the attack against the home area network of the SGI, through definition and generation of routine device behaviors. Any observed de-

viation from the defined normal profile is labeled as a malicious attack. A number of datasets are generated by varying the percentage of devices in a single record that contribute towards identifying a data sample as a attack.

In Chapter 5, we study Support Vector Machines for detection of device implant attacks based on the various datasets modeled in Chapter 4. The detection accuracy of the proposed approach is evaluated in terms of true positives and false positives.

In Chapter 6, we propose a Self-Organizing Map (SOM)-based approach for data clustering, for facilitating classification of SGI data into either the normal class or the anomalous class. A detailed analysis of the proposed is carried out for specific parameters and varying map sizes.

## CHAPTER 2

# LITERATURE REVIEW

The advent of the Smart Grid presents a new paradigm that aims to solve many of the shortcomings of the traditional grid while also providing several unique functionalities to the consumers. The Smart Grid is envisioned to be a completely automated infrastructure that will require little or no human intervention. This will be made possible by the integration of latest information and communications technologies (ICT) into the power grid. However, this integration of technology also raises several concerns about the protection of the Smart Grid against cyber-attacks. In this chapter we provide a brief overview on the topic of network security and outline various vulnerabilities of the Smart Grid. A survey of the security measures available in literature is provided and several machine learning techniques that can be potentially used to develop unique strategies for securing the Smart Grid are highlighted in this chapter.

## 2.1 Network Security

The advent of the internet and improvements in networking technologies over the years has provided many possibilities for sharing information and interconnecting different parts of the world. Today the worldwide network hosts data from private individuals, commercial entities, government organizations and military setups that require access to their data 24/7. Business organizations have the ability to quickly and easily share information with their partners, divisions and customers internationally. Governments today share information with their citizens through the internet and have replaced traditional methods with internet-based information sharing systems. This ease of availability and accessibility of sensitive information also makes it vulnerable to internet-based cyber-attacks. Attackers are able to take advantage of the open source nature of the Internet to carry out attacks on critical infrastructures while leaving no evidence of their malicious activities.

Information security is defined as the process of protecting data from unauthorized access, use, modification, tempering, or disclosure [12]. When designing a strategy to secure the network it is important to take into account all aspects of the network. For instance, just securing the end devices in a network does not protect the network from cyber-attacks. It is also equally important to secure the channel of communication between the devices. Hackers could intercept the exchange of data between devices over a channel, modify it and insert it back into the channel leading to a security breach. Hence, securing the channel through

means of encryption techniques is just as important as securing the end devices.

### 2.1.1 Types of Network Attacks

Without proper security measures in place a network always remains a potential target for a variety of network attacks. While there are several types of attacks, most of them can be classified into the following categories [13]:

- *Eavesdropping*: This type of attack takes place when an attacker is able to monitor or listen to traffic in transit. Such attacks are relatively easy to carry out as TCP/IP being an open architecture sends data in cleartext format. The attacker only needs to have access to a traffic capture tool in order to capture the on-going data.
- *Data Modification*: Once the data has been eavesdropped, it can be easily modified leading to falsified information. This attack becomes significant especially in cases where data being transferred includes sensitive information like confidential company data and billing information. The attacker is able to modify the data without the sender gaining any knowledge about the modification taking place.
- *Identity Spoofing (IP Address Spoofing)*: The Internet is an IP based network and every host in it is uniquely identified using an IP address. This makes it possible for an attacker to assume the IP address of a valid entity resulting in identity spoofing. The attacker is then able to modify, reroute, or delete data of the original user.

- *Password-Based Attacks:* Traditional applications do not always guarantee the security of user credentials as it travels through the network for verification. As such this information can be easily eavesdropped by an attacker. On obtaining the username and password of the authentic user the attacker also inherits the access privileges of the user which the attacker can use to illegally obtain information about legitimate users and computer names, invalidate network configuration and alter user data.
- *Denial-of-Service Attacks:* A denial of service refers to an attack that aims to make an authentic service unavailable to its intended users. This can be achieved by exhausting all the resources of the target device so that it is unable to reply to genuine requests or by overloading the network to the extent that it causes the network to shutdown.
- *Compromised-Key Attack:* A key is a shared secret code that is used to interpret secret information that is communicated between two network entities. Although difficult it is not impossible for an attacker to gain access to this key. The key when with the attacker is known as a compromised key, which the adversary could use to obtain further keys thereby gaining access to other secured communications.
- *Sniffer Attack:* A sniffer is a software tool or device that is able to monitor and log traffic passing over a digital network. Although sniffers are primarily meant to be used as troubleshooting tools, they can also be used by attackers to carry out malicious activities. Sniffers are used by hackers to capture



packets and extract sensitive information like username and password.

- *Application-Layer Attack*: An application-layer attack leads to malfunctioning of system applications or the operating system running on a server. An attacker that carries out such an attack has the ability to modify or delete the operating system, use system resources to create and replicate viruses several times and disable security controls leading to further attacks.

It is important to note that there is no such thing as a 100% secure network and no single scheme that ensures one security solution for all scenarios. Different situations may demand different levels of network security depending on the criticality of the information being shared through the network.

## 2.2 Intrusion Detection

In an information and communication technology (ICT) setup, an intrusion is defined as any attempt to break-in to the system by either an external agent, or by an unauthorized insider. The process of detecting such malicious activities is called *Intrusion Detection* and an *Intrusion Detection System (IDS)* is a software or hardware based tool that monitors network traffic in order to detect such malicious activities and reports them accurately to the proper authority.

The efficiency of an IDS is evaluated based on the following parameters described in [14]:

- *Accuracy*: Accuracy is defined as the ability of an IDS to correctly identify

intrusions and minimize the number of false alarms. An IDS is tagged as inaccurate if it wrongly detects a genuine event in the medium as anomalous or intrusive.

- *Performance*: The rate at which audit events are analyzed by an IDS is used to determine its performance. A poorly performing IDS will lack the ability to detect attacks in real-time.
- *Completeness*: Completeness is the ability of an IDS to detect all attacks. On the other hand, incompleteness takes place when an attack is executed and the intrusion-detection system is unsuccessful in detecting this attack.
- *Fault Tolerance*: An important requirement for the proper functioning of an IDS is for the system itself to be resilient to attacks. This is because majority of the IDSs run on top of commercially accessible operating systems or hardware, which are easy targets for attacks.
- *Timeliness*: An intrusion-detection system needs to be able to relay information in a timely manner in order to halt further penetration of the attack and to allow the responsible personnel to take precautionary measures to prevent the system from being compromised.

Most intrusion detection techniques can be generally classified into one of two classes, namely, *Anomaly Detection* and *Misuse Detection*. Anomaly detection is based on the principle that an intruders characteristics will significantly vary from that of a authorized user and thus such behavior could be easily identified. A pre-

requisite for this approach is to train the intrusion detection scheme with normal network traffic behaviour patterns. Although, anomaly detection techniques are capable of detecting both known as well as unknown attacks, they suffer from a large number of false alarm rates. On the other hand, misuse detection techniques use pattern matching schemes to match incoming traffic with known patterns of attacks and classify it as an attack.

IDSs can be additionally divided into host-based IDSs, distributed IDSs, and network-based IDSs based on the location of knowledge used for classification. A host-based intrusion detection system (HIDS) is defined as a system that monitors a computer system on which it is installed and is responsible for detecting attacks against this host only; distributed IDSs are designed to detect attacks in scenarios involving multiple hosts and thus obtain information from both the hosts and the network that interconnects these hosts. Finally, Network-based IDSs collect data from network traffic. Also because the system does not rely on specific attacks to be trained it is much easier to maintain. Common approaches for intrusion detection include *Statistical Models* and *Machine Learning Techniques* [15].

### **2.2.1 Statistical Models**

Statistical-based systems (SBIDs) work by defining what a normal traffic is and then classify everything else as anomalous. A SBID system continues to learn network traffic patterns as long as it is active. The longer a SBID system is able to last, the more accurate is its classification. The system analyzes network

traffic and tags every packet with an anomaly score and generates an alert if a packet score is found to be above a certain threshold. Due to its ability to detect unknown attacks the SBID system is considered much more efficient than rule based detection systems. However, because the SBID system is dependent on the knowledge gained from the regular patterns of network traffic, the system may not prove to be viable in networks where the traffic is quite diverse and continuously changing. Another drawback of the system is its learning speed. It may take days or even weeks to gain an acceptable level detection accuracy.

In [16], statistical models were applied for detecting novel attacks against networks. In the proposed work network activity models were used to detect denial of service and probe attacks. The KolmogorovSmirnov test was used for application models to prove the statistical difference between normal and attack telnet connections in the DARPA dataset.

In [17], Wang et al. used the difference between the number of SYN and FIN packets, which was modeled as a stationary random process, to detect SYN flooding attacks. The authors then used the CUSUM algorithm to look for a change-point in the time series corresponding to the sum of received SYN packets and thus detect the SYN flooding attacks. The drawback of such an approach is that an alarm can be set off only when there is a significant change in the aggregated series.

An anomaly detection technique based on Principal Component Analysis (PCA) was proposed in [18]. In the proposed approach, normal traffic behavior is rep-

resented by  $k$ -subspace achieved through PCA and anomalies are denoted by the outstanding  $(n - k)$  subspace. The method proposed claims inferior false alarm rates along with network-wide anomaly detection.

### 2.2.2 Machine Learning Techniques

A primary shortcoming of signature based intrusion detection techniques is their inability to adapt to new intrusion types. The signature database needs to be manually updated for every new intrusion discovered. Even if an attack is discovered and its signature is used to develop a detection prototype, the system would become obsolete by the time it comes into production. These limitations have led to an increased interest in the field of using data mining for intrusion detection. Data mining (also known as Knowledge Discovery) is the process of locating beneficial and recently unknown patterns in large volumes of information. Data mining techniques can be demarcated in terms of their model functions and representation, preference criterion, and algorithms [19]. The field of machine learning is a subset of data mining which is concerned with the development of intelligent algorithms that learn autonomously through experience. Examples of such algorithms include data mining programs that discover general rules in large data sets and information filtering systems that automatically learn users interests [15]. Machine learning techniques can be classified into two types, namely, supervised and unsupervised machine learning algorithms [20]. The aim of supervised learning algorithms is to assign labels to

unknown samples using knowledge gained from the training phase where labeled feature vectors are used as input for training. In contrast, unsupervised learning schemes are trained using unlabeled samples. Common data mining techniques [15] that have been used for intrusion detection are presented in this section.

### **Inductive Rule Generation**

The RIPPER System is probably the most popular technique representing this class. RIPPER [21] is a fast rule learning technique that generates concise rule sets. The system uses a set of rules and patterns that can prove realistic for classification for network traffic. The rule set generated by the system is simple and allows multiple rule sets to be created and used with a meta-classifier.

### **Genetic Algorithms**

Genetic algorithm (GA) is a Artificial Intelligence (AI) based search technique that is inspired from the principles of evolution and natural selection [22]. The concept of GAs was first initiated by John Holland and his aides in the early 1970s. In computer security applications, it is mainly used for finding optimal solutions to a specific problem. The algorithm usually begins with a group of chromosomes that is arbitrarily selected and is used to characterize the problem to be resolved. A chromosome is represented using either bits, characters, or numbers. A fitness function is used to select chromosomes with superior fitness values that results in a improved solution. To determine the fitness level of

a chromosome an evaluation function is employed. The natural processes of reproduction and mutation of species during the evaluation phase are simulated using two intrinsic operators, namely, mutation and crossover. In the mutation process, the value of a given gene is randomly changed from its current state to a completely new one. The crossover method proceeds through the combination of two parent chromosomes that produces two descendant chromosomes. The combination of chromosomes may take place in one of two ways:

- The two parents are duplicated unaltered as offspring.
- The two parents are randomly joined to create offspring.

GA or GP based systems exhibit superior performance when compared to other systems because they can be easily trained multiple times. The best population obtained from the previous iteration can be simply used as initial population for the next loop. However, the operations this time are performed on new data. This implies that the entire process is inherently flexible.

Bankovic et al. [23] proposed a intrusion detection system that is based on the serial combination of two genetic algorithms and promises low computational overhead. The first IDS simply behaves as a linear classifier that separates normal instances from possible attacks. To minimize the high number of false-positives produced from the first IDS, a second system based on if-then rules is implemented that refines the output from the first stage. Incremental genetic algorithms are used to train both the systems. For linear classification, every chromosome in the population is composed of four genes. The first three

chromosomes represent the coefficients of the linear classifier and the fourth one signifies the threshold value. Alternatively, each rule in the rule-based system is represented by a 3-gene chromosome and the population size used here is much smaller than that chosen for the first system. The use of two different system enables each system to be trained independently of the other.

The fitness function in Genetic Algorithm is used to determine the fit chromosomes that define the next generation population through the crossover and mutation processes. Alim Al Islam et al. [24] recommended a fitness function that is based on the accuracy-existence-occurrence structure. A higher accuracy factor points to a strong rule to detect theft whereas a higher value of existence indicates that the rule matches more in the dataset. The value of existence is only needed for random selection from the population while both accuracy factor and the occurrence are to be included in the fitness function. The authors propose the use of accuracy factor and occurrence in a weighted form. A highly secured network demands a higher weight for accuracy and a faster security implementation implies a higher weight for occurrence.

An intrusion detection system called ID-SOMGA was proposed by Folorunso et al. in [25] which is composed of two other algorithms: *Self Organizing Migrating Algorithm (SOMA)* and *Genetic Algorithm (GA)*. The resultant hybrid algorithm is able to tackle small as well as large population sizes. SOMGA is used to design rules that can detect attack instances only. The obtained rules are tried on historical connections and are later used to identify suspect network



traffic during future network traffic scans. If a rule is successful in identifying an anomalous connection, a bonus point is awarded to it and a penalty is likely otherwise. As compared to an IDS with GA, the proposed approach display much slower performance but provides a very small ratio of false positive rate.

Another approach that utilizes genetic algorithm for intrusion detection was presented in [26]. In the proposed approach normal instances are distinguished from anomalous instances based on simple rules derived from network traffic. Theses rules are typically formulated in form of *if (condition) then (act)*. The *condition* is used to represent a match between current network connection and the rules in IDS and the *act* defines the actions to be performed which may include include reporting of alerts to system supervisor or blocking the connection attempt.

### **Fuzzy Logic**

Fuzzy Logic was first introduced in 1965 by Lotfi A. Zadeh, professor for computer science at the University of California in Berkeley [27]. Fuzzy Logic (FL) is a multi-valued logic that is used to define in the middle values like yes/no, true/false etc. A fuzzy set forms the basic building block of fuzzy logic and is considered to be an improvement over the mathematical set. For example the temperature a cup of tea is known to fall in the range of 0 to 100 degree Celsius. A cup of tea with temperature 70 degrees is considered hot (1) and a cup of tea with a temperature of 20 degrees is considered cold (0) and therefore the

decision in both these cases is definite. However, a cup with a temperature of 50 degrees might be considered hot by some while others might take it to cold. This uncertainty in classification is referred to as fuzziness. A fuzzy set enables such classifications to be successfully carried out. Fuzzy logic readily extends its support to the field of intrusion detection as it helps in overcoming the fuzziness in differentiating between normal and anomalous events. The elimination of insignificant inputs results in a much simpler problem and also provides gains in speed and classification accuracy.

In [28], the authors proposed the integration of fuzzy logic and genetic algorithms for intrusion detection. Fuzzy logic is used to include quantitative parameters in intrusion detection, whereas genetic algorithm is used to find best fit parameters of introduced numerical fuzzy function. Another work in this direction was investigated in [29]. The fuzzy sets in this approach are normalized to fit within the boundary of 0.0 to 1.0. The genetic algorithm is used to create rules for both normal and anomalous behavior. Rules are represented as complete expression tree and the tree structure is used to represent and classify data. This approach of integration has however not proven to be very effective against port scans.

Abadeh et al [30] tried to improve fuzzy rules by using local search operators to search their neighborhood. Instead of generating the initial population randomly, a training data sample is randomly selected, and the most compatible combinations of antecedent fuzzy sets is determined. A heuristic method is used to determine the consequent part. If the consequent part confirms the class label

of data samples the rule is kept else the the generation process is repeated again.

## **Neural Networks**

An artificial neural network (ANN), also popularly known as neural networks, is a computational mode inspired by biological neural systems. A neural network consists of a huge number of highly interconnected neurons that collaborate with each other towards solving a categorical problem. Each neuron is made up of a summing element and an activation function. The output from each neuron is in turn used as input to all the next layer neurons.

A back propagation neural network was proposed by Ghosh et al. in [31]. The performance of the introduced neural network was found to be equivalent to that of a basic signature matching system. The Base Security Module (BSM) is used to create the training set out of the captured strings of events. The proposed neural network behaves as an anomaly detector if the training set is composed of strings pertaining to normal behavior and as a misuse detection module if the strings correspond to attack scenarios.

Ryan et al. [32] defined a contemporary detection method using neural networks that provides off-line anomaly detection. The Neural Network Intrusion Detection (NNID) anomaly detection system exploits the distribution of commands performed by a user to identify him/her as a genuine user. Upon collection of data, training is implemented using a back propagation neural network and each user is identified based on the training data. A user is tagged as anomalous if the

neural network places low confidence in its decision. A maximum activation value of below 0.5 is an indication of an anomaly. In another approach [33], the two class problem of classifying normal and attack instances was resolved using three and four layer neural networks. Based on experiments conducted a classification accuracy of above 99% was reported.

Michailidis et al. [34] employed PSO to optimize the weights of multilayer perceptrons (MLPs). The principle used to evolve the weights is similar to the one used by genetic algorithms. The proposed algorithm is tested on a small (under-sampled) subset of the KDD Cup 99 data set. Their findings are comparable to other applications of MLPs. Their approach detects more Probing and U2R attacks, but at the expense of a higher FPR. However, it is not understood whether this due to the use of PSO to train the MLPs, or due to the under-sampling.

### **Support Vector Machine**

A Support vector machine (SVM) is a binary classification algorithm that plots the training vectors in high dimensional feature space, separating the set of training vectors into two separate classes. The training samples close to a decision boundary constitute the support vectors. The SVM also enables users to balance between the number of misclassified samples and the width of a decision boundary through a parameter called penalty factor. Although, SVMs are capable of achieving a high detection rate, they also give rise to a high false

positive rate. To address this issue Tian et al [35] proposed a new technique for anomaly detection that combines One-Class SVMs and PSO techniques. The Receiver Operating Characteristics (ROC) curve evaluates parameters selection, the area under the ROC curve (AUC) represents the fitness of each particle and the PSO algorithm is used to search the global ideal SVM parameters. This technique achieves a high true positive rate (TPR) with a low false positive rate (FPR).

Ma et al. [36] proposed a hybrid algorithm that combines binary particle swarm optimization (BPSO) and support vector machine (SVM). To optimize the dataset feature selection and SVM parameters optimization, the linearly decreasing weight strategy and random mutation are employed to update velocities in BPSO. The task of SVM in the setup is to differentiate between normal and anomalous behavior. The modified BPSO is used to obtain the best particle position quickly throughout the search space, which cooperates with SVM for evaluating the fitness of the corresponding particle. This combined approach allows for the selection of optimum features and parameters at the same time.

In [37], a time-based inductive machine (TIM) was proposed that is able to provide information about a users behavior pattern. One general application of the TIM is discovery of patterns in a sequence of events that are temporally correlated. A logical interpretation mechanism called inductive generalization is used to generate and modify rules which are derived from the temporal patterns. In the scope of intrusion detection, the scheme is used to predict the next event

based on information gathered about a sequence of events. Here, rules represent the behavioral patterns of a group of users or a single user.

### **Immunological Based Techniques**

The computer immunological approach [38] is inspired from the immune systems ability of differentiating between self and non-self. Both self and non-self are represented as strings of length  $l$  in this system. Any string of length  $l$  that does not match any string belonging to the pool of self-strings is considered as non-self. The differentiation process consists of generating a random string of length  $l$  and then checking if there is a matching string for it in the pool of self-strings. On successful match, the string is discarded; else it is marked as a detector. This is a simple approach but has high time complexity which increases exponentially with the number of self-strings.

The artificial immune system (AIS) proposed by Kephart [39] is the first attempt towards emulating the human immune system (HIS) for intrusion detection. The main objective of the proposed approach is the the automatic detection of computer viruses and worms. The viruses are initially detected by the system using either fuzzy matching or through the use of integrity monitors. While fuzzy logic is used for pattern matching with available signatures of viruses, an integrity monitor is used to report any changes in key system binaries and data files. In order to confirm the identification of a program as a virus and to reduce the number false positives, a set of dummy programs are maintained in

the system whose main objective is to get infected. If any such dummy program gets infected, it is an indication that the detected program is indeed a virus. Consequently, signatures of the virus from the infected program are extracted and communicated with the neighbouring systems. In addition the infected binaries are cleaned and returned to the original state.

### **Clustering Techniques**

Clustering is the categorization of related entities into different sets. In the context of a dataset, clustering is defined as the splitting of the dataset into subgroups or clusters such that records in each subgroup are related to each other in some way. The applications of data clustering are many including data mining, image analysis, pattern recognition and machine learning. In particular, clustering finds its use in the field of intrusion detection due to the need for clustering anomalous actions together thereby separating it from legitimate data. The clustering approach is known to be superior to other classification techniques as it does not require the use of a labeled data set for training.

A self-organizing map (SOM) or self-organizing feature map (SOFM) is a data visualization system that decreases the magnitudes of data through the use of self-organizing neural networks. It was proposed by Professor Teuvo Kohonen of the Neural Networks Research Center (Helsinki University of Technology, Finland) in the early 1980s. Major components of a SOM include the sample data, the vector weight and the training algorithm. The vector weight is itself

composed of two parts: 1. its data, and 2. its natural location. The SOM is a unsupervised learning method, which implies that no human interference is required during the learning process and that little knowledge is required about the features of the input data. An input vector is presented to the SOM network of neurons and a single neuron is determined as a winning neuron based on its similarity to the input vector. The weight of the winning neuron is updated to make it more closer to the input vector. A SOM represents the input space of the training samples in a 1 or 2-dimension map. At the end of the SOM training process similar data items are grouped together that enables data visualization. SOM was used by Lichodzijewski et al. [40] to develop a host-based intrusion detection system that attempts to makes the process of intrusion detection completely autonomous. The proposed system uses pattern discovery to model the behavior of a common user. A two level SOM architecture is used where the first level is composed of three maps and the second level is represented by one network. Each of the three maps in the first level is used to signify a single feature, the first map models the location from which the connection is established, the second map represents the user account which is used to execute the log-in process and the final map imitates the connection type. In general, the first level is used to summarize the features in the three input domains with respect to time. The second level gathers input from the first level and merges the values received from the three different maps at level one to provide an overall report on user activity. This outcome is then used by the network manager to



classify a particular session as either normal or anomalous.

In order to handle the vast amount of alerts generated by IDS devices Lifan et al. [41] proposed a Self-Organizing Map (SOM) based hybrid alert clustering method that also incorporates particle swarm optimization (PSO). Binary particle swarm optimization (BPSO) and mutual information (MI) are used for selection of relevant features, while SOM is employed to cluster the dataset. PSO is used to evolve the weights for SOM to improve the clustering result. The proposed scheme when compared with the canonical SOM model for the 2000 DARPA dataset, achieves a higher clustering accuracy rate for the connection records which represent DOS, Probing and normal records respectively.

## **2.3 Security Implications of Smart Grid**

It is generally convenient to presume that emerging problems can be easily overcome using existing approaches. Unfortunately, this approach has not always proven to be fruitful in the past due to the unique challenges posed by new domains. The Smart Grid replacing the its highly acknowledged and dependable traditional grid, presents a number of new security challenges, in addition to other existing ones, that necessitate innovative methodologies to the field of cyber security.

The Smart Grid is composed of a variety of small, resource-constrained devices such as Smart Meters, sensors and supervisory control and data acquisition (SCADA) devices that are hampered by limited battery and processing power.

As such it is vital to design security solutions for the Smart Grid that take into consideration these constraints.

Price information, meter data, and control commands constitute the major portion of the information exchanged between heterogeneous devices of the Smart Grid. As such any security scheme designed for the Smart Grid needs to ensure at minimum the following [42]:

- *Confidentiality of Power Usage:* Lack of security measures for meter data can lead to leakage of information about the usage patterns for individual appliances. This loophole can be exploited by intruders simply by monitoring the appliances.
- *Integrity of Data, Commands, and Software:* It is important to safeguard the integrity of price information as incorrect low prices inserted by an attacker can result in a sudden jump in the utilization of electricity. This is because several appliances would concurrently switch on to take advantage of this newly advertised low price. In addition, integrity of software is important because infected software can compromise different grid components.
- *Availability Against DoS/DDoS Attacks:* Denial-of-service (DoS) attacks aim to make resources unavailable to their legitimate users and can lead to resource exhaustion by sending fabricated requests to a server, and distributed DoS (DDoS) attacks deny access to authentic users from using a specified network resource like Smart Meter and appliances.

## 2.4 Vulnerable Smart Grid Domains

The Smart Grid is a combination of several complex components each of which operates in harmony with the others. Therefore, compromise of any one component can lead to the disruption of the entire Smart Grid. Major security vulnerabilities for the Smart Grid can be generally categorized into one of the the following categories [43]:

- PCS Security
- Smart Meter Security
- Power System State Estimation Security
- Smart Grid Communication Protocol Security

### 2.4.1 PCS Security

Process Control Systems (PCS) are employed by the Smart Grid to monitor and control physical aspects of the electrical power grid. PCSs were traditionally designed to run in isolated environments and hence did not necessitate any built-in security measures. However, the large scale nature of the Smart Grid implies that these PCSs if used without modification will create multiple entry points into the network which can potentially be used to execute malicious actions. There are a variety of PCSs. The most widely known PCS for the electrical power grid is the Supervisory Control And Data Acquisition (SCADA) system.

An Intrusion Detection System (IDS) that can support different PCSs was pro-

posed by Valdes and Cheung in [44]. Although most PCSs had no security measures designed to handle security breaches, they were still being used in corporate networks in practice. This posed security threats because PCSs could now be manipulated by outside connections through the corporate domain. The motives behind attacking the PCS could range from causing financial loss or damage to expensive equipment to causing physical injuries. Since the PCS configuration is known to remain static and the traffic flow through it can be easily modeled, a model-based IDS was suggested for intrusion detection. In addition to the model-based approach, a signature-based approach is used in order to detect known attacks.

Jiaxi et. al. [45] contributed two different cyber security assessment methods that allow the level of cyber security risk of a system to be defined. The two methods are: probabilistic assessment and an integrated approach. The probabilistic assessment approach assigns a vulnerability index to the cyber systems based on the combined probability of occurrence of an incident and the probability of a resulting incident. In the integrated approach the extremity of security risks is used to classify them into one of five different classes. The degree of cyber security risk is determined using the obtained probabilities and a formula.

### **2.4.2 Smart Meter Security**

A Smart Meter is generally a electrical meter that is installed at customer premises and is used to provide real-time energy consumption information to the customers.

The captured energy consumption information is communicated by Smart Meter to the energy suppliers. Smart Meters also allow for a much more advanced modeling of the power usage requirements as compared to the traditional power meters. It is important to secure the Smart Meters as falsified readings sent from the Smart Meter to the supplier can result in improper billing, and fabricated power usage approximations. Because Smart Meters are typically installed at consumer locations they are within easy reach of malicious users who may attack the Smart Meter either for monetary gains or to cause financial loss to the legitimate end-user. Integrity and confidentiality are the two most important security objectives in this domain as it is important to maintain the correctness of Smart Meter readings.

A scheme for compressed meter reading in Smart Grid was proposed by Li et. al. in [46]. The compressed meter reading concept is unique as it enables the access point to differentiate the reports from a number of simultaneously transmitting Smart Meters. When compared to the carrier sense multiple access (CSMA) technique, the simultaneous access technique provides relatively uniform delays. The use of a random sequence in the compressed sensing provides a higher level of privacy and integrity of the meter reading.

In [47], a privacy preserving protocol using zero knowledge proof for Smart Meters was proposed. The zero knowledge proof is used to ensure the correctness of the bill without disclosing any details about the consumption data.

A specification based IDS that performs real time screening of the traffic between

meters and access points at different layers of the OSI model was proposed in [48]. To ensure proper operation of the system in scenarios of malicious meters and DoS (Denial of Service) attacks the authors define a set of four monitoring rules. The formulated rules are tested in a realistic AMI environment and a formal verification of the specifications and monitoring operations is carried out at the application layer.

To verify the correctness and accuracy of Smart Meter measurements an echo method was suggested in [49]. The proposed method allows energy suppliers to echo the power readings they receive from Smart Meters back to the customers. These data echoes can in turn be used by the end-users to confirm the integrity of the Smart Meter measurements. The work in [49] provided a encryption method for encoding the data echoes. The encrypted readings could only be decrypted using the original Smart Meter readings. If an echoed reading cannot be decoded with the original reading then this meant the two readings are distinct.

An approach to handle intrusion threats aimed at the advanced metering infrastructure (AMI) was presented in [50]. The authors proposed the use of specification based IDS as it offers better accuracy when compared to signature-based IDS. In addition specification based systems do not need experimental data to sense intrusions and due to limited number of protocols implemented by Smart Meters would prove to be highly beneficial for ensuring the Smart Grid environment. However, such systems introduce significant overhead and are also costly to implement.

### 2.4.3 Power System State Estimation Security

In order to maintain the stability of the the electrical power grid, the Smart Grid is required to control the physical properties of the electrical power system. To achieve this the Smart Grid must model the current state of the power system so that it can make informed decisions and take appropriate actions on them. The state estimation model is considered to be a part of the PCS. Thus it is important that the security objectives that are defined for PCSs are also applied to state estimation system. The power system state estimation model is a tool used by the Smart Grid PCSs to model sensor and agent data.

The contribution of the work in [51] shows the impacts of performing a false-data injection attack on the Smart Grid. The impact of the attack is measured in terms of monetary gain by manipulating pricing of the electrical market. The work also shows that it is possible to perform this attack without being detected. The attacker does need to know the pricing model that is being used by the system to carry out this attack successfully.

A light-weighted pattern matching scheme for detection of attacks in the Smart Grid was proposed in [52]. A number of malicious attacks specific to the Smart Grid are identified that include:

- *Consumer Device Implant Attacks:* Any attack where a fake device implanted in the Smart Grid infrastructure is identified as a legitimate device by the system.
- *Meter Implant Attacks:* The purpose of this attack is to place a hoax meter

with malicious software to alter meter reading resulting in either a increase or a reduction of billing amount for the consumer.

- *Black Hole Attacks:* A black hole attack occurs in the network when a data concentrator halts forwarding of all meter readings to their rightful destinations i.e., control centers.
- *Malicious Hand-held Terminals:* The transfer of viruses from handheld devices to smart components such as Smart Meters and concentrators can cause considerable disruption to normal operations of the Smart Grid.

The graph neuron (GN) algorithm is utilized to identify malicious or misbehaving devices in the network and to take appropriate actions which may include replacement of the infected device. Two pre-defined thresholds are used to classify a device as a malicious one: Upper threshold (UT) and lower threshold (LT). UT is the maximum generated reading by a device and LT is the minimum. Any observed reading for a device that does not fall under the boundary [LT, UT] is concluded to be generated from an infected device.

#### **2.4.4 Smart Grid Communication Protocol Security**

The Smart Grid is a combination of different communication environments each of which introduces its own protocol and security requirements to meet the multi-dimensional nature of the resultant communication infrastructure. Examples of these requirements include performance parameters like very low latency and high data throughput. Because the Smart Grid is completely dependent on its commu-



nication infrastructure to ensure its smooth functioning, it is imperative to design robust security measures for the Smart Grid communication protocols. Many of the major Smart Grid functionalities are rendered useless if no communication is available.

A set of design principles for creating authentication protocols in the Smart Grid was proposed in [53]. These design principles were created by altering the Internet-based principles to achieve stronger security objectives that are relevant to the Smart Grid. Zhang and Gunter [54] proposed a secure multi-cast protocol that can be used for communication in the Smart Grid. The objective behind using multi-cast is its ability to utilize bandwidth more efficiently. The proposed secure multi-cast communication protocol is unique because it is able to automatically determine group membership. Group membership can be automatically determined as the protocol is application-aware. The communication protocol was implemented using IPSec as it achieves low latency for medium sized networks.

**CHAPTER 3**

**FUZZY-BASED**

**OPTIMIZATION FOR**

**EFFECTIVE DETECTION OF**

**SMART GRID**

**CYBER-ATTACKS**

In this chapter, we propose a pattern matching technique, wherein the smart devices of a consumers household of a home area network exchange personal electricity consumption readings with each other through a structured hierarchy, at fixed intervals of time. We have formulated an equation to balance the tradeoff between the frequency of inter-device communication and accuracy in attack detection in the presence of a variable number of implanted devices. We present

a fuzzy logic-based optimization approach towards achieving a realistic tradeoff between attack detection rate and cost of inter-device communication. The reason to introduce fuzzy logic for detection of attack is that security for smart grid itself includes fuzziness. Device implant attacks occur when a device is either implanted within the home area network to generate fictitious readings for delivery to the smart meter, or to forbear from actual communication with the smart meter. Hoax devices implanted within the vicinity of a home area network (HAN) are capable of generating malicious electricity utilization data for subsequent delivery to the smart meter, thereby resulting in incorrect electricity usage bill for a client. The Werners Fuzzy operator [55] is applied to find the optimal balance between frequent communication of attack detector nodes for detecting smart grid attacks when the formulation for attack detection proposed is implemented, and the actual accuracy in attack detection. The resulting values of system parameters obtained through the fuzzy-based formulation have been analyzed subsequently.

The rest of the chapter is organized as follows. Section 3.1 presents an overview of the device implant attack. The attack detection scheme and the system parameters involved thereof are described in Section 3.2. A summary of the fuzzy based optimization is presented in Section 3.3. We present our simulation results and analysis in Section 3.4.

### 3.1 Device Implant Attack

The ability of smart grid to minimize the electricity utility bill for end-users is one of its main advantages and is highly praised. However, this very communication infrastructure also can act as a platform from which a large number of malicious attacks can be launched. Although, many malicious attacks have been identified in the literature, with the capability of disrupting the smooth functioning of the smart grid setup, the newness of the technology has meant that not all vulnerabilities of the SGI have been discovered yet. As a result, there is a lack of substantial proof to clearly identify malicious activity within the smart grid communications, as opposed to routine activity. However, due to readily available hacking tools, a malicious activities can be easily executed against any online resource that is part of the Internet.

A consumer device implant attack is defined as an attack by a malicious user wherein a malicious device is installed within the SGI home area network for the following purposes:

- To generate fictitious readings for delivery to the smart meter, and
- To emulate an existing device operational in the network, and abstain from actual communication with the smart meter [52].

Such an attack is generally initiated through the implantation of one or several hoax consumer devices within a particular home area network. These implanted devices will generate falsified data for subsequent delivery to the smart meter. The motives behind such an attack may be to cause financial harm to the legitimate

end-user by increasing his electricity usage bill beyond the actual figure or the attack may be carried out the end-user himself to reduce his electricity bill. The user in the latter case will try to benefit through a less-than average electricity bill to be settled at the end of the month.

## **3.2 Attack Detection Scheme**

In the absence of shared secret keys or the public key infrastructure to provide secure communication both between the consumer devices as well as between the devices and the smart meters, the confidentiality of any information exchange within the smart grid infrastructure is not achievable. As a result, such an attack can affect the confidence of consumers on a particular service provider, or may affect the profitability of the provider incurred through incorrectly reduced electricity bills.

### **3.2.1 Steps for Attack Detection**

The proposed technique is based upon distributed definition and confirmation of SGI device readings through a predefined communication pathway for each device. Each device  $i$  in the home area network is programmed to communicate with exactly two other devices in the network, in close proximity to device  $i$ . As illustrated in Figure 3.1, the legitimate SGI devices of the home area network are programmed to communicate with exactly two other neighboring SGI devices, to exchange their respective power consumption readings, at fixed intervals of time.

In addition, rogue devices that are implanted into the network will try to disrupt such communication through their individual attempts to transmit falsified device readings to the smart meter.

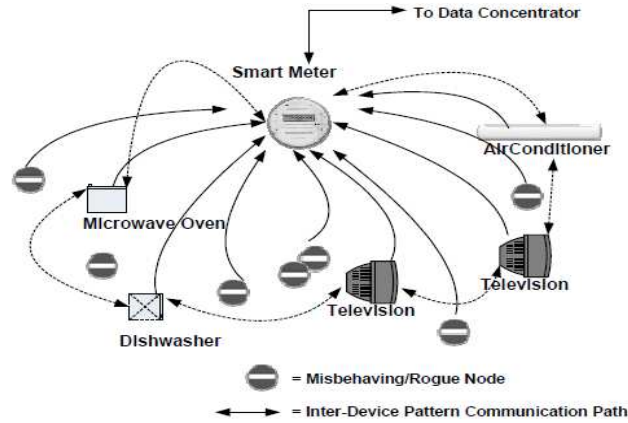


Figure 3.1: The proposed device implant attack detection scheme.

We model the device readings as subpatterns, and we refer to this regular exchange of device readings as pattern exchange. At the end of the pattern exchange process during a given time frame of length  $L$ , see Figure 3.2, each device will consist of a 3-tuple comprising of its personal device reading ( $reading_i^t$ ), and two neighboring device readings =  $(reading_{i-1}^t, reading_{i+1}^t)$ .

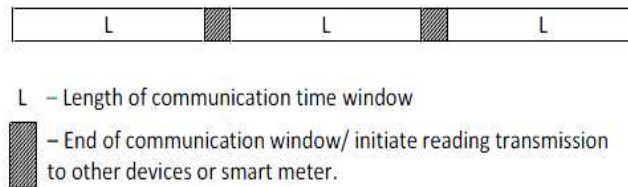


Figure 3.2: Smart devices communicate at regular intervals.

Following is the sequence of steps that outline the attack detection scheme:

- *Initialization:* During this phase, which is executed only once at time of network initialization, all SGI devices operational within a home area network are pre-configured with addresses of two other devices in their close vicinity. As a result, a device  $i$  will form a communication link with devices  $i - 1$  and  $i + 1$ , respectively. In addition, based on selected parameters of the scheme, namely, values of  $N$ ,  $\gamma$ ,  $C_C$ , and  $C_C$ , and Equation 3.3, the time window length  $L$ , is fixed. This time window length defines the frequency of inter-device communication required for attaining a high degree of accuracy in attack detection, imposing minimal resource overhead in terms of communication delays, imposed. An alternating communication parameter (Alternating Sequence(i)) is configured within each device. This parameter essentially restricts the device from communication during Phase 3 below in any two consecutive time windows. The purpose of such practice is to cut-down the communication overhead both in terms of resource usage as well as delays incurred by the scheme in half.
- *Pattern Exchange:* As part of the detection scheme execution, individual devices record their electricity usage at the end of every time window, and communicate their readings with their two respective peer devices. As a result, a 3-tuple reading is stored within each device at the end of a given time window.
- *Smart Meter Communication:* During this phase of execution, the pattern

tuples of electricity usage reconstructed within each SGI device are communicated, in alternate manner, with the smart meter. The alternating criteria is based on skipping alternate time windows, so as to ensure that individual SGI devices do not communicate with the smart meter, to share their reconstructed patterns, in any two consecutive intervals of time.

- *Attack Identification:* When a smart meter receives the 3-tuple device readings from  $\frac{N}{2}$  devices at the end of each window of time, these readings are considered genuine and stored. An attack is identified if multiple device readings are received for the same SGI device within a given frame of time. Such a scenario alludes towards the presence of implanted devices attempting to disrupt SGI operations through communication of incorrect device readings to the smart meter. In such scenarios, the device with multiple reported readings is identified and the consumer is appropriately informed to take necessary mitigation action.

The first step towards securing the smart grid infrastructure is through the detection of the malicious attack. In particular, device implant attacks require that the detection scheme be able to identify the misbehaving devices of the network in a timely and accurate manner, so as to be able to mitigate the effects of the attack, upon successful detection. Identification of patterns of routine SGI device readings by the smart meter is one such approach towards confirming routine network activity. On the contrary, a misbehaving device attempting to convey incorrect readings to the smart meter will be identified through the



reconstruction of the patterns exchanged between alternating SGI devices and the smart meter. The readings of individual devices of a given home area network constitute the information that must be verified for correctness. In Figure 3.3, we provide a sequence of steps executed by the proposed scheme, for device implant attack detection.

```

1. Initialisation
for  $i=1$  to  $N$  do
    | Select peer devices  $i-1$  and  $i+1$ 
    | Generate  $L$  based on Eqn. 3
    | if  $device\_ID \% N = 0$  then
    | | Alternate_sequence = 0
    | end
    | else
    | | Alternate_sequence = 1
    | end
end
Current =  $\neg$ (Current)
2. Pattern Exchange
for  $i = 1$  to  $N$  do
    | Communicate with neighboring devices  $i-1$  and  $i+1$ 
    | to reconstruct pattern  $\{p_i^t, p_{i-1}^t, p_{i+1}^t\}$ 
end
3. Smart Meter Communication
for  $i = 1$  to  $N$  do
    | if  $Alternate\_sequence(i) = Current$  then
    | | Communicate with Meter
    | end
end
4. Attack Detection Outcome
for  $i = 1$  to  $\frac{N}{2}$  do
    | if  $multiple\_response\_received(i) = true$  then
    | | Tag  $i$  as implanted.
    | end
end

```

Figure 3.3: The proposed attack detection scheme.

### 3.2.2 Optimal Parameter Selection

Following is a list of parameters of the proposed device implant detection scheme:

- $F$  is the frequency of communication between the SGI devices for pattern

exchange and reconstruction,

- $C_I$  is defined as the cost (overhead) imposed on the home area network through incorrect device reading verification,
- $C_C$  is defined as the cost of operating a device implant attack detection scheme, through added messages exchanged,
- $N$  is the overall number of devices active in the network,
- $\gamma$  is defined as an estimate on the number of implanted devices within the network.

The frequency of inter-device communication for pattern exchange and reconstruction at the end of each interval of time of length  $L$ , is defined through the parameter  $F$ . Selecting higher values of this parameter implies that the scheme requires frequent exchange of device readings. In other words, a higher value of  $F$  will imply a shorter time window length  $L$ , where the value of  $L$  is lower bound by the minimal time required for a home area network with  $N$  devices to successfully execute the pattern exchange process. On the contrary, selecting smaller values of  $F$  will lead to less frequent exchange of device readings, and less frequent reconstruction of patterns, for delivery to the smart meter. As a result, the timely detection of an attack may be affected. Through Equation 3.1, an elaboration on the total cost associated with the proposed device implant detection scheme is provided.

$$TotalCost(C) = \frac{\gamma C_I}{F} + \frac{FC_C}{N} \quad (3.1)$$

As the network size  $N$  increases, the frequency of inter-device communication  $F$  will also tend to increase, as more number of devices must communicate with each other. Moreover, increasing  $N$  implies reduced distances between the devices, and therefore a reduction on the per-device communication overhead. As the number of malicious implanted devices ( $\gamma$ ) increases, the frequency of inter-device communication increases so as to ensure timely and accurate identification of malicious device readings before the scope of damage through such an attack increases. The value of  $C_C$  is considered to be the cost associated with the communication delay between any two devices. Therefore, a large value of  $C_C$  implies that the distance between the two communicating devices is high, therefore lesser frequency of inter-device communication will ascertain that on-device energy resources are not rapidly depleted.  $C_I$  is the cost associated with loss of system resources owing to adversary presence  $\gamma$ . In order to reduce the effective cost, in terms of  $F$ , incurred by the attack on the smart grid infrastructure, Equation 3.1 is differentiated with the resulting expression (given by Equation 3.2), equated to zero:

$$TotalCost(C) = \frac{-\gamma C_I}{F^2} + \frac{C_C}{N} \quad (3.2)$$

As a result, an optimal frequency of inter-device communication is yielded so as to both effectively detect the attacks and to avoid a drastic increase in the imposed overhead on the system through repeated pattern exchange between the devices.

This optimal frequency expression for the given scenario is given by:

$$F = \sqrt{\frac{C_I}{C_C} \times N \times \gamma} \quad (3.3)$$

The above equation provides the minimal value of  $F$  to attain a high level of accuracy in attack detection with a minimum number of messages exchanged between the SGI devices.

### 3.2.3 Multi-Objective Approach to Attack Detection

The cost ratio ( $\alpha = \frac{C_I}{C_C}$ ) directly impacts the frequency of inter-device communication and hence the attack detection rate. Thus it is essential that the value of  $\alpha$  is optimized so that an ideal communication cost is achieved so as to both efficiently identify attacks and to avoid a radical increase in the forced overhead on the system due to regular pattern exchange between the devices. Hence the problem of achieving this tradeoff can be viewed as a multi-objective decision-making problem. To achieve the optimal value of  $\alpha$  we propose a fuzzy-based decision making scheme and Werner compensation operator is adopted to aggregate the two objectives to generate a compromise solution which is both compensatory and Pareto-optimal.

### 3.2.4 Werners Operator

Werners [55] “*fuzzy and*” and “*fuzzy or*” are two compensatory operators used in solving multi-objective problems. The operators have an advantage of being

directly proportional to the compensation rate. In addition, they have produced equitable results in existing applications. The compensatory “*fuzzy and*” and “*fuzzy or*” operators introduced by Werners [55] combine the minimum and maximum operator respectively with the arithmetic mean. The combination of these operators leads to enhanced results with respect to empirical data and allows compensation between the membership values in the aggregated sets. Based on these advantages we used Werners “*fuzzy and*” operator to achieve a trade-off between the attack detection rate and cost of inter-device communication.

The “*fuzzy and*” operator is represented as [56]:

$$\mu_{and}(\mu_A(x), \mu_B(x)) = \gamma \cdot \min(\mu_A(x), \mu_B(x)) + \frac{(1 - \gamma)[\mu_A(x) + \mu_B(x)]}{2} \quad (3.4)$$

$x \in X, \gamma \in [0, 1]$

The “*fuzzy or*” operator is represented as [56]:

$$\mu_{OR}(\mu_A(x), \mu_B(x)) = \gamma \cdot \max(\mu_A(x), \mu_B(x)) + \frac{(1 - \gamma)[\mu_A(x) + \mu_B(x)]}{2} \quad (3.5)$$

$x \in X, \gamma \in [0, 1]$

For  $\gamma = 1$  the “*fuzzy and*” becomes the minimum operator and the “*fuzzy or*” behaves as the maximum operator. While for  $\gamma = 0$  the arithmetic mean is obtained for both operators [56].

### 3.3 Fuzzy Logic

Fuzzy Logic is used to mathematically represent human reasoning by allowing in-between values to be defined between logical evaluations such as true/false, on/off, yes/no, etc. A fuzzy set forms the basic building block of fuzzy logic and is considered to be an improvement over the mathematical set. For example the temperature a cup of tea is known to fall in the range of 0 to 100 degree Celsius. A cup of tea with temperature 70 degrees is considered hot (1) and a cup of tea with a temperature of 20 degrees is considered cold (0) and therefore the decision in both these cases is definite. However, a cup with a temperature of 50 degrees might be considered hot by some while others might take it to cold. This uncertainty in classification is referred to as fuzziness. A fuzzy set enables such classifications to be successfully carried out. This can generally be done by allowing several or even infinite number of values between the set boundaries. An example of such a set is the unit interval  $[0, 1]$ , where an element which has number 1 assigned to it belongs to the set and an element with number 0 assigned to it does not belong to it. All the other elements are described by real numbers between 0 and 1 corresponding to their membership in the set. The larger the real number assigned to an element, the higher is its membership. A linguistic variable is analogous to an algebraic variable with the difference that instead of taking numbers as values it takes words or sentences as values.

The basic structure of a fuzzy inference system consists of three conceptual components: a rule base, a database and a reasoning mechanism [57]. The rule base

is a collection of fuzzy rules and the database is used to define the membership functions in these fuzzy rules. Finally, the reasoning mechanism is used to derive a conclusion based on inference from the rules. For our scheme we consider two linguistic variables, namely Total Cost and Detection Rate. We are interested in achieving a low total cost for a high detection rate. Our objective is to find the optimal value of the cost ratio that will yield the best tradeoff between the two parameters being investigated. To achieve this we define the following rule:

Rule: **IF** a solution X has *low communication cost* AND *high attack detection rate*, **THEN** it is an optimal solution

The membership function for the frequency of communication between the attack detection nodes is calculated based on the equation presented by Werners [55]:

$$Membership(F_i) = [\frac{-1}{maxF}(F_i - minF)] + 1 \quad (3.6)$$

The membership function of attack detection rate is calculated based on the following equation suggested by Werners [55]:

$$Membership(DR_i) = \frac{1}{maxDR}(DR_i - minDR) \quad (3.7)$$

The membership values for total cost and detection rate are computed in such a way that we maximize the detection rate while minimizing the total cost.

## 3.4 Results and Analysis

### 3.4.1 Simulation parameters

Simulations were performed to obtain an optimal value for  $\alpha$  that will provide an accepted level of communication rate while at the same time resulting in a high detection rate. In Table 4, we provide the parameters selected for running the simulations.

Parameter	Value
Cost ratio( $\alpha$ )	0.1 to 1.0
Number of devices (N)	10 to 30
Number of Implant devices ( $\gamma$ )	0.25 to 1.0

Table 3.1: Simulation Parameters.

### 3.4.2 Simulation Results

The simulator for testing the effectiveness of the proposed fuzzy based scheme was implemented in JAVA. The simulations were carried out for varying values of  $\gamma$  and its effect on the detection rate was analyzed. In addition, the total number of devices,  $N$ , was varied to study its effect on the detection rate and it was found that for  $N = 10, 20$  and  $30$  the results are almost identical and therefore we only present results for  $N = 30$ .

In Tables 3.2 - 3.5, we present the membership values for the two parameters (total cost and detection rate): MemF and MemDR, as well as the overall



membership denoted by OM. For varying values of the cost ratio, the total cost is calculated based on Equation 3.3.

It can be inferred from the obtained results that an increase in the number of implanted devices ( $\gamma$ ) results in a higher cost of communication ( $F$ ) as the frequency of communication is increased between the devices. However, increasing values of  $\gamma$  also result in better attack detection rate and thus higher MemDR values.

$\alpha$	<b>F</b>	<b>DR</b>	<b>MemF</b>	<b>MemDR</b>	<b>OM</b>
0.1	0.866025404	15.8113883	1	0	0.25
0.2	1.224744871	22.36067977	0.934507085	0.065492915	0.282746457
0.3	1.5	27.38612788	0.884252604	0.115747396	0.307873698
0.4	1.732050808	31.6227766	0.841886117	0.158113883	0.329056942
0.5	1.936491673	35.35533906	0.804560492	0.195439508	0.347719754
0.6	2.121320344	38.72983346	0.770815548	0.229184452	0.364592226
0.7	2.291287847	41.83300133	0.73978387	0.26021613	0.380108065
0.8	2.449489743	44.72135955	0.710900288	0.289099712	0.394549856
0.9	2.598076211	47.4341649	0.683772234	0.316227766	0.408113883
1.0	2.738612788	50	0.658113883	0.341886117	0.420943058

Table 3.2: Simulation Results for  $N = 20$  and  $\gamma = 0.25$ .

It can be observed from Table 3.2 that maximum overall membership is obtained at a cost ratio ( $\alpha = 1.0$ ). Although we achieve a high detection rate of 50, this high detection rate is obtained for a high level of cost ratio. This implies that when there are a few number of malicious devices as compared to the number of normally behaving devices it is difficult for the proposed scheme to differentiate between the two. Hence to achieve a large detection rate the scheme needs to

monitor a larger number of communications between the devices.

$\alpha$	F	DR	MemF	MemDR	OM
0.1	1.224744871	22.36067977	0.934507085	0.065492915	0.282746457
0.2	1.732050808	31.6227766	0.841886117	0.158113883	0.329056942
0.3	2.121320344	38.72983346	0.770815548	0.229184452	0.364592226
0.4	2.449489743	44.72135955	0.710900288	0.289099712	0.394549856
0.5	2.738612788	50	0.658113883	0.341886117	0.420943058
0.6	3	54.77225575	0.610391326	0.389608674	0.444804337
0.7	3.240370349	59.16079783	0.566505905	0.433494095	0.466747048
0.8	3.464101615	63.2455532	0.525658351	0.474341649	0.487170825
0.9	3.674234614	67.08203932	0.48729349	0.51270651	0.493646745
1.0	3.872983346	70.71067812	0.451007102	0.548992898	0.475503551

Table 3.3: Simulation Results for  $N = 20$  and  $\gamma = 0.5$ .

As the number of implanted devices is raised from 0.225 to 0.5 there is an improvement in the overall membership from 43% to 49%. However the cost ratio is still high at 0.9. This again indicates that higher number of inter-device communications are needed for effectively detecting attacks.

$\alpha$	<b>F</b>	<b>DR</b>	<b>MemF</b>	<b>MemDR</b>	<b>OM</b>
0.1	1.5	27.38612788	0.884252604	0.115747396	0.307873698
0.2	2.121320344	38.72983346	0.770815548	0.229184452	0.364592226
0.3	2.598076211	47.4341649	0.683772234	0.316227766	0.408113883
0.4	3	54.77225575	0.610391326	0.389608674	0.444804337
0.5	3.354101966	61.23724357	0.545741447	0.454258553	0.477129276
<b>0.6</b>	3.674234614	67.08203932	0.48729349	0.51270651	0.493646745
0.7	3.968626967	72.45688373	0.433545046	0.566454954	0.466772523
0.8	4.242640687	77.45966692	0.383517214	0.616482786	0.441758607
0.9	4.5	82.15838363	0.336530047	0.663469953	0.418265023
1.0	4.74341649	86.60254038	0.292088479	0.707911521	0.39604424

Table 3.4: Simulation Results for  $N = 20$  and  $\gamma = 0.75$ .

For  $\gamma = 0.75$  we observe a much better cost ratio as compared to the first two cases. The same overall membership is achieved for  $\gamma = 0.75$  as is achieved with  $\gamma = 0.5$  with a much lower cost ratio of 0.6. This implies that as the number of implanted devices in the network outnumber the normally behaving devices a higher detection rate is achieved by observing fewer communications.

$\alpha$	<b>F</b>	<b>DR</b>	<b>MemF</b>	<b>MemDR</b>	<b>OM</b>
0.1	1.732050808	31.6227766	0.841886117	0.158113883	0.329056942
0.2	2.449489743	44.72135955	0.710900288	0.289099712	0.394549856
0.3	3	54.77225575	0.610391326	0.389608674	0.444804337
0.4	3.464101615	63.2455532	0.525658351	0.474341649	0.487170825
0.5	3.872983346	70.71067812	0.451007102	0.548992898	0.475503551
0.6	4.242640687	77.45966692	0.383517214	0.616482786	0.441758607
0.7	4.582575695	83.66600265	0.321453856	0.678546144	0.410726928
0.8	4.898979486	89.4427191	0.263686692	0.736313308	0.381843346
0.9	5.196152423	94.86832981	0.209430585	0.790569415	0.354715292
1.0	5.477225575	100	0.158113883	0.841886117	0.329056942

Table 3.5: Simulation Results for  $N = 20$  and  $\gamma = 1$ .

The analysis from previous table is further confirmed in Table 3.5 as we can observe we achieve a high detection rate of 63% for a relatively cost ratio of 0.4. Although the detection rate for  $\gamma = 1$  is slightly less than that for  $\gamma = 0.75$  we achieve this tradeoff for a much lower cost ratio.

To meet the objective of the optimization problem we locate the highest value of OM in Tables 3.2 - 3.5. It can be observed that for lower values of  $\gamma$  ( $=0.25, 0.5$ ), it is preferable to use a higher value of  $\alpha$ , equal to 1. This implies that higher total cost needs to be detected to achieve a reasonably higher detection rate. For example,  $\gamma = 0.5, \alpha = 1.0$  yields a detection rate of nearly 71%.

For networks with larger number of implant devices ( $\gamma$ ), higher values of overall membership are achieved with relatively lower cost ratios. For example,  $\gamma = 0.5, \alpha = 0.9$  yields a detection rate of nearly 50%. It can be inferred from the above tables that as the intensity of rogue devices ( $\gamma$ ) in the network is increased the

frequency of communication among devices increases and thus does the communication cost. This enables an acceptable detection rate to be achieved before the scope of the damage through an attack increases and because this detection rate is achieved at a lower  $\alpha$  implies that the attack is detected well before the end of the time window.

In this chapter we proposed a noble approach based on fuzzy logic for multi-objective optimization between the two parameters involved in the detection scheme for detecting device implant attacks, namely, Cost of Communication and Attack Detection rate, by varying the value of the cost ratio ( $\alpha$ ). From experimental results obtained it can be concluded that the best value for  $\alpha$  lies between 0.4 and 0.6 for all combinations of parameter values tested.

## CHAPTER 4

# SMART GRID DEVICE BEHAVIOR DATASET

The lack of accurate data about current smart grid system deployments means that researchers may make inaccurate assumptions which may lead to incorrect results. Therefore, we propose a dataset in this section that models the attacks against the home area network of the SGI, through definition and generation of routine device behaviors. Any observed deviation from the defined normal profile is labeled as a malicious attack. We merge the normal behavior data samples with randomly generated malicious device behavior data, to form a dataset. The labeling of data samples is done through the definition of distinct rules. The malicious data samples are generated based on the premise that implanted hoax devices or compromised appliances of a home area network (HAN) are capable of generating malicious electricity utilization data for subsequent delivery to the smart meter, thereby resulting in incorrect electricity usage bill of a client. The generated

dataset will allow us to accurately model the device implant attack for the smart grid. Subsequently, we propose the use of intelligent schemes like Support Vector machine (SVM) and Self-Organizing Map (SOM) for facilitating classification of the generated SGI data into either the normal class or the anomalous class.

## 4.1 Dataset Generation

A dataset is modeled based on the operating patterns of home appliances in a typical household network of the smart grid infrastructure. The modeled dataset consists of 108,000 data samples. Each data sample in turn consists of 10 appliances, each of which is represented by three parameters (features). These features include device id, randomly generated energy values belonging to device operation during a given time frame of a day, and a difference category. Table 4.1 presents the power ratings for typical household devices that we have considered for our work.

Device	Power Rating (Watts)
Air Conditioning	1500
100 Watt bulbs	100
Microwave Oven	1700
Dish Washer	1000
Washing Machine	1000
Kettle	3000
Iron	2000
Desktop PC	300
Laptop	100
Television	600

Table 4.1: Power Ratings for Common Household Devices.

In addition, each data sample also consists of a label to classify the data sample as either normal (representing routine home network operations), or anomalous, based on the extremity in the readings (too high or too low), when observed collectively. Table 4.2 highlights the normal energy consumption in Kwh for devices listed in Table 4.1. The formula for estimating energy consumption is provided in Equation 4.1

$$DailyEnergyConsumption(kWh) = \frac{Wattage \times HoursUsedPerDay}{1000} \quad (4.1)$$

Device	Power Rating (Watts)	Energy Consumption(kWh)
Air Conditioning	1500	1.5
100 Watt bulbs	100	0.06
Microwave Oven	1700	1.7
Dish Washer	1000	1
Washing Machine	1000	1
Kettle	3000	3
Iron	2000	2
Desktop PC	300	0.3
Laptop	100	0.1
Television	600	0.6

Table 4.2: Energy Consumption (kWh) of Home Appliances.

It may be noted that not all appliances/devices are active during all time frames



of a day. Therefore, we intuitively describe a combination of devices that are simultaneously active during any given time interval of a particular day. The overall energy consumption during an interval is taken as the aggregated sum of energy consumed by all active devices.

Random values are generated for each device identified as being active during a time interval. An inactive device is given an energy feature value of 0 which indicates a don't care, and this value is ignored during determination of the sample class. The randomly generated energy values are then compared with the estimated normal energy consumption values in Table 4.1 and a label is assigned to each device. The label assigned may be extreme, marginal or medium, based on the difference between the two energy values (expected and actual):

- *Marginal*, if the difference is  $\leq 15\%$ ,
- *Medium*, if difference is between 15% - 35%, and
- *Extreme*, if the difference is  $\geq 35\%$ .

This criterion is applied to all dataset samples and the labels assigned are then later used to classify each row as either normal or anomalous.

A device is known to behave normally if it is labeled as either marginal or medium in the previous step. As such, percentages of devices are used for defining a particular dataset sample. A total of 5 datasets were thus generated based on the criteria for labeling the dataset samples. For example, one dataset that was used in our experiments had samples labeled as normal if 25% (4 out of 10) devices exhibited normal energy values, and was labeled as an attack instance otherwise.

Table 4.3 highlights the distribution of normal and attack instances in the dataset variants used for our simulations.

<b>Dataset Type</b>	<b>Normal Rows</b>	<b>Attack Rows</b>
25%	79036	28964
35%	79017	28983
45%	76884	31116
55%	43443	64557
65%	39834	68166

Table 4.3: Basic Dataset Characteristics.

A snapshot of several data samples for the 25% dataset is presented in Table 4.4. The data rows presented are in the normalized form where each device reading is labeled as either 51 (marginal), 52 (medium) or 53 (extreme). The entire row is either tagged as 50 (normal) or as 100 (attack). It can be observed from Table 4.4 that device 4 (dishwasher) is only active at 07:00 am and therefore has a random energy value of 0.54 generated for it. The device is assigned a label of 53 for this time slot as the randomly generated energy of 0.54 kWh is different from the actual power rating of 1 kWh by more than 35%. The device is assigned value 0 for all other time slots indicating that the device is probably not in use during the other time slots. In addition it can be inferred that the data row for 06:00 am is labeled as an attack (100) because 3 out of 3 active devices are labeled as extreme (53). It is important to note that when assigning an overall label to a row only active devices are monitored for their labels while devices which

are inactive during that time slot (i.e., have label 0 assigned to them) do not contribute towards determining the data row label.

06:00	1	0.97	53	2	0	0	3	0.61	53	4	0	0	5	0	0	6	0	0	7	0.7	53	8	0	0	9	0	0	10	0	0	100
07:00	1	1.44	51	2	0	0	3	0	0	4	0.54	53	5	0	0	6	0	0	7	0	0	8	0	0	9	0.1	51	10	0	0	50
08:00	1	1.25	52	2	0	0	3	0	0	4	0	0	5	0	0	6	2.59	51	7	0	0	8	0	0	9	0	0	10	0.54	51	50
09:00	1	1.11	52	2	0	0	3	0	0	4	0	0	5	0.16	53	6	0	0	7	0	0	8	0	0	9	0	0	10	0	0	50
10:00	1	0.54	53	2	0	0	3	1.22	52	4	0	0	5	0	0	6	0	0	7	0	0	8	0	0	9	0	0	10	0.41	52	50
11:00	1	0.22	53	2	0	0	3	0	0	4	0	0	5	0	0	6	0	0	7	0	0	8	0	0	9	0	0	10	0.17	53	100
12:00	1	1.03	52	2	0	0	3	0.23	53	4	0	0	5	0	0	6	0.47	53	7	0	0	8	0.26	51	9	0	0	10	0	0	50
13:00	1	0.8	53	2	0	0	3	0	0	4	0	0	5	0	0	6	0	0	7	0.86	53	8	0	0	9	0	0	10	0	0	100

Table 4.4: Sample Dataset Rows.

It can be concluded from Table 4.3 that most datasets are imbalanced in favor of either class. This implies that the identification accuracy of the model will be affected since the learning algorithm will encounter more samples from the dominant class of the dataset in question. For instance, the 65% dataset is heavily biased towards the attack class with nearly twice as many attack rows as the normal rows. In order to minimize the effect of the bias, the 55% dataset is identified as the best dataset out of the five generated since it has the lowest imbalance between the two classes. Although, the dataset may not ideally reflect existing real Smart Grid networks, we believe it still can be applied as an effective testbed to help researchers compare different intrusion detection methods for the Smart Grid.

## 4.2 UMass Smart\* dataset

The UMass Smart\* dataset is a part of the Smart\* project [58] and is composed of power measurements and heterogeneous sensory information collected by sensors installed in 3 real households. The dataset contains information about home electricity usage parameters such as average household electricity usage every second, as well as electricity usage at each circuit and nearly every plug load, electricity generation data from on-site solar panels and wind turbines, outdoor weather data, temperature and humidity data in indoor rooms, and, finally, data for a range of important binary events, e.g., at wall switches, the HVAC system, doors, and from motion sensors.

The UMass Smart\* dataset consists of 44640 data samples and each sample is composed of 17 features, namely, `TimestampUTC`, `insideTemp`, `insideHumidity`, `outsideTemp`, `windChill`, `intervalAvgWindChill`, `outsideHumidity`, `apparentTempF`, `windDirection`, `windDirectionDegrees`, `windSpeed`, `intervalAvgWindSpeed`, `windGustDirectionDegrees`, `rainRate`, `dailyRain`, `dailyRainMM` and `class`.

One apparent difference between the proposed dataset and the Smart\* dataset is the number of parameters monitored by a single device. In the proposed dataset the only attribute assigned to a device is the randomly generated power level at which the device operates and the device is tagged as normal or malicious accordingly. On the other the Smart\* dataset monitors 17 different parameters.

<b>Dataset Type</b>	<b>Normal Rows</b>	<b>Attack Rows</b>
25%	24187	23350
35%	22329	22311
45%	22408	22232
55%	22482	22158
65%	22376	22264

Table 4.5: Basic Smart\* Dataset Characteristics.

A major drawback of the Smart\* dataset is that the data samples are unlabeled. As such all samples are assumed to exhibit normal behaviour. To introduce anomalous samples into the dataset in order to make it consistent with the proposed datasets varying number of features of the Smart\* dataset were modified and datasets similar to Table 4.3 were obtained. Basic characteristics of the modified Smart\* datasets are presented in Table 4.5.

## CHAPTER 5

# SUPPORT VECTOR MACHINE (SVM) BASED SG INTRUSION DETECTION

A Support Vector Machine (SVM) is a supervised machine learning system that has been widely used for intrusion detection. In this chapter we describe the application of support vector machine to the detection of attacks at the HAN level of Smart Grid hierarchy. We employ SVM due to its good generalization ability of the learning model. This implies that good accuracy can be achieved even with relatively smaller training datasets when SVM is used for classification. Another advantage of SVM is its ability to handle a large number of features. In addition SVM also ensures high accuracy for classification of future data from the same allotment to which the training data belongs [59]. Experimental results obtained confirm high accuracy of attack detection and insignificant false positive

rates for our proposed approach.

## 5.1 Support Vector Machine (SVM)

Support vector machines (SVMs)[59] are supervised knowledge based systems that project the input vectors in feature space of large dimensions, assigning each vector a label. SVMs categorize data by defining a group of support vectors that belong to the set of training inputs that outline a hyper plane in the feature space [60]. SVMs have been used for both two-class and multi-class classification.

### 5.1.1 Two-Class Classification

In order to classify a two-class linearly separable data, SVM creates a hyperplane that separates the binary classes of the the specified dataset with the largest margin that provides best generalization ability [59]. Generalization ability is the ability of the classifier to ensure classification accuracy on training data as well as accuracy in classifying future data. A margin is used to decide the degree of separation between two classes. Figure 5.1 illustrates an optimal hyperplane for a two-class classification, where two different classes are represented: normal class (circles) and attack class (squares).

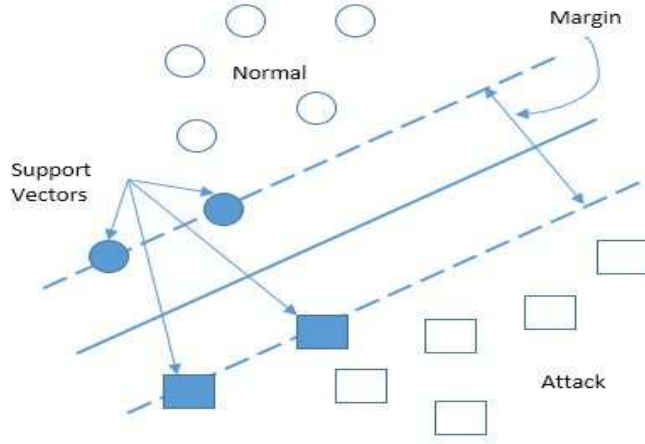


Figure 5.1: Optimal hyperplane for a two-class input space.

The aim of SVM here is to create a linear boundary (solid line) that expands the margin (space between dashed lines) between the two different classes. The data points that fall closest to the margin (shaded squares and circles) are known as *support vectors*. The classifier is defined based on these support vectors. The model presented in Figure 5.1 is only expected to work when the data that can be linearly separated in the feature space.

Mathematically, the linear boundary can be expressed as [61]:

$$w^T x + b = 0 \tag{5.1}$$

The classification problem using the training set can be estimated using a function  $f : \mathbb{R}^n \mapsto \{\pm 1\}$ . We present the normal class with  $x \in normal, y = 1$  and the attack class with  $x \in attack, y = -1$ ;  $\{x_i, y_i\} \in \mathbb{R}^n \times \{\pm 1\}$ . If the training data



can be linearly separated then there exists a pair  $(w, b) \in \mathbb{R}^n \times \mathbb{R}$  such that

$$w^T x + b \geq +1 \text{ for all } x \in \text{normal} \quad (5.2)$$

$$w^T x + b \leq -1 \text{ for all } x \in \text{attack} \quad (5.3)$$

The decision function is given by

$$f(w, b)(x) = \text{sign}(w^T x + b) \quad (5.4)$$

where  $w$  is the weight vector and  $b$  is the bias. The inequality constraints from Equations 5.2 and 5.3 can be collectively represented as:

$$y(w^T x + b) \geq 1 \text{ for all } x \in (\text{normal} \cup \text{attack}) \quad (5.5)$$

The aim of the classifier is to now to optimize the above by splitting the data with the hyperplane that provides the largest margin. Therefore the learning problem considering the constraints in Equation 5.5 can be formulated as:

$$\text{minimize } \frac{1}{2} * \| w \|^2 \quad (5.6)$$

If SVM is unable to separate the binary classes, it uses a kernel function to plot the input vectors into  $n$ -dimensional feature spaces. There are several available choices for the kernel function including linear, polynomial, or Gaussian. The

margin that splits the data points defines the number of parameters used by SVMs. Hence SVMs do not involve any reduction in the number of features and are free from the problem of over-fitting. Another major benefit of SVMs is that the prospect of generalization errors is quite small. After classification is completed, an appropriate optimization process can be applied for identification of additional features if necessitated by the application [62].

### **5.1.2 Multi-Class Classification**

Although, Support Vector Machines were initially meant to be used for classification of two-class data (also known as binary classification), researches have recently strived to extend the applicability of SVM to multi-class input space as well. Presently, there exist two main SVM methodologies for classification of multi-class data, namely, one-against-all and one-against-one methods [63]. The one-against-all approach works by assembling and merging several binary classifiers. On the other hand, one-against-one formulates all data into one optimization problem. Further details on multi-class classification can be obtained from [64].

## **5.2 Results and Analysis**

In the proposed approach, each IDS at the HAN level will incorporate the SVM scheme in order to detect attacks and stave off intrusions. All experiments were carried out using the Weka Software [65]. The SVM algorithm is executed in two phases: training phase and testing phase.

### **5.2.1 Weka Tool**

Weka [65] is a pool of several freely accessible data mining and machine learning algorithms, including data pre-processing, grouping, and association rule extraction. It is an open source application written in Java that is freely available under the GNU general public license agreement. It provides a graphical interface that allows for quick set up and operation. The input to the Weka tool is in the form of a flat file where each data object is described by a fixed number of attributes that usually are of either alpha-numeric or numeric type.

### **5.2.2 Training**

In the training phase the SVM algorithm is provided with the labeled input (i.e., first 70% data samples of the entire dataset). The output from this stage includes the margin, the support vectors, the alpha values and the weights. For our data samples, label 50 is assigned to a normal record and label 100 is assigned to an attack record. At the end of this phase a training model for the data is obtained. The training set is comprised of 75600 instances and each instance is defined by 31 attributes. Each instance is also labeled as either normal or attack and the liner function is employed.

### **5.2.3 Testing**

In the testing phase, we provide the test dataset (i.e., remaining 30% of data samples in the dataset) without the class labels. This phase uses the classification

model created at the end of the training phase. The results obtained from the testing phase are presented in Table 5.1.

<b>Parameter</b>	<b>25%</b>	<b>35%</b>	<b>45%</b>	<b>55%</b>	<b>65%</b>
Instances	3240	3240	3240	3240	3240
Attributes	31	31	31	31	31
Detection Accuracy	90.929%	91.2809%	90.1173%	90.7037%	91.0123%

Table 5.1: SVM Testing Results.

It can be observed from Table 5.1 that SVM provides efficient classification of the datasets with over 90% detection rate for every dataset.

<b>Dataset</b>	<b>a(normal)</b>	<b>b(attack)</b>	<b>% correct</b>
25	22415	1264	94.7
	1675	7046	80.8
35	22518	1266	94.7
	1559	7057	81.9
45	21611	1413	93.9
	1789	7587	80.9
55	11454	1604	87.7
	1408	17934	92.7
65	10379	1532	87.1
	1380	19109	93.3

Table 5.2: SVM Confusion Matrix.

The confusion matrix was calculated (Table 5.2) for each of the modeled dataset and it can be observed that the true positive rate in detecting both normal and attack samples is quite high for all datasets. For example, the top-left item in the confusion matrix for the 25% dataset implies that 22415 of the confirmed

“normal” test samples were predicted as “normal”. This implies that 94.7% of the actual “normal” examples were recognized properly. Similar results are obtained for the 35% and 45% datasets. However, from 55% dataset it can be inferred that the true positive rate for the normal samples reduces by a small margin while the true positive rate for the attack samples shows a significant improvement. For instance, the results for the 65% dataset indicate that 87.1% of the normal samples are identified correctly whereas 93.3% of attack rows are correctly identified as attacks which is an improvement of more than 10% from the true positive rate obtained for the 45% dataset.

Therefore, it can be concluded from the obtained results that as the number of malicious devices in the HAN level increases the proposed scheme is able to detect these devices with high rate of accuracy while involving minimum overhead for the detection scheme.

## CHAPTER 6

# SELF-ORGANIZING MAP (SOM) BASED ATTACK DETECTION FOR SMART GRID

The communications infrastructure of the SGI is prone to several malicious attacks identified in the recent past. Customer-specific electricity readings are communicated up the SGI hierarchy from consumer devices to centralized servers through intermediary devices such as smart meters and data concentrators/aggregators. In this chapter, we propose a Self-Organizing Map (SOM)-based approach towards training and testing of centralized SGI devices to qualify them for identifying anomalies accurately. The proposed scheme is capable of detecting anomalous readings within a consumers household, with reasonable accuracies. SOM was

used as an unsupervised learning algorithm [66] because of its simplicity and efficiency in classifying data. As compared with other learning techniques, SOMs provide higher speed and faster conversion rates in processing real-time data that is being regularly exchanged between different hierarchical levels in the Smart Grid.

## 6.1 Self-Organizing Maps (SOMs)

The Self-Organizing Maps proposed by Teuvo Kohonen, a professor at the Academy of Finland, is a artificial neural network approach for evaluating and envisioning n-dimensional data in significantly smaller magnitudes of 1 or 2 dimensions [67]. A SOM is trained using unsupervised learning, which implies that no human intervention is required during the learning phase and that little knowledge is essential about the features of the input data. SOMs have been applied to a wide range of areas ranging from pattern recognition to image analysis as well as intrusion detection.

### 6.1.1 The SOM Structure

A SOM structure is generally constructed by placing nodes (also called neurons) in a two-dimensional grid or lattice called SOM map (see Figure 6.1). The neurons in a SOM map can be organized in both matrix and hexagonal topology. In addition, each node  $i$  in the SOM map is linked to a n-dimensional weight vector,  $x_i = [x_{i1}, x_{i2}, \dots, x_{in}]$ , where the dimension of n is identical to that of the input vectors. The input layer to the the SOM is a collection of the vectors representing features

of the problem under investigation. The output layer is the two-dimensional arrangement of nodes that is directly related to the input layer [67].

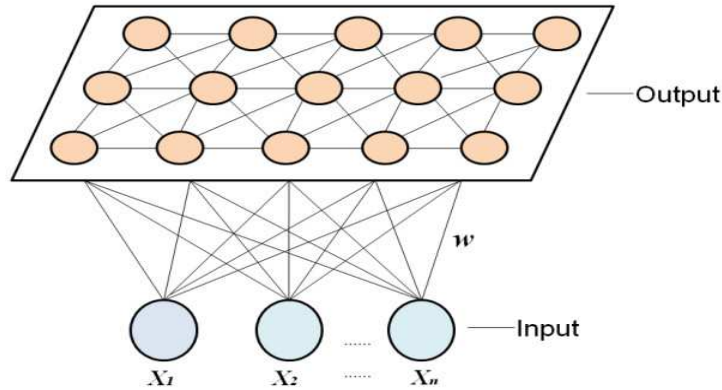


Figure 6.1: Typical SOM Architecture.

At the end of the learning phase, similar nodes in the grid are clustered together whereas dissimilar nodes are separated from each other. A neighborhood function is used to determine the level of connectivity between the neurons. The most frequently employed method to determine the neighborhood in SOM is the Gaussian neighborhood approach.

### 6.1.2 Preprocessing

In the datasets proposed in Chapter 4 each data sample is defined by 32 features. Out of the 32 features 31 features are used in this work as we remove the time-stamp feature from the datasets as it does not contribute in the classification of a sample. Since SOM can only deal with data in numeric format, alphanumeric values in the dataset such as class label are enumerated to fit the training criteria. A normal label is enumerated as 50 and an attack label is enumerated as 100. After enumeration has been performed, normalization is then used to ensure that no



single feature is more influential than any other feature in determining the training result. Therefore, all dataset values are normalized to fall within the unit interval  $[0,1]$ . The normalization is done using the root mean square (RMS) method.

### 6.1.3 SOM Training

The first step towards training the SOM is the initialization of weight vectors for all the grid neurons. Generally the initialization can be done using any of the three approaches, namely, random, sample or linear initialization. In all training iterations, an input vector  $v$  is arbitrarily drawn from the training set and its match with every weight vector in the SOM lattice is determined. A winner neuron or the Best-Matching Unit (BMU) is chosen based on the level of similarity between the neuron vector and the input vector. The most commonly used measure to determine the similarity between the two vectors is the Euclidean distance. Thus, a neuron that exhibits minimum distance to the input vector is chosen as the winner neuron. The next step in the training phase is to minimize the distance from the input vector to the BMU and its topological neighbors. All the neurons that fall within the neighborhood of the BMU are updated while others are left unaltered. The neighborhood radius is assigned a large value initially and then allowed to decay exponentially in every iteration. This allows the map to be ordered globally. The SOM map settles to a certain 'good fit' state after all iterations (equal to the number of data samples that were introduced), are completed.

Following are the steps involved in the SOM training algorithm [68]:

- **Step 1:** Create a SOM weight matrix. The SOM map size and topology are defined here.
- **Step 2:** Initialize the weights of all matrix nodes with randomly values in the interval  $[0,1]$ .
- **Step 3:** For every input vector  $v$ ,

- **3.1** Compute the distance between the current input vector and the weight vector of every node. The Euclidean distance between the vectors is given as:

$$Dist = \sqrt{\sum_{i=0}^n (v_i - w_i)^2} \quad (6.1)$$

Where  $v$  is the input vector representing the current input and weight vector of the neuron is given by  $w$ .

- **3.2** Choose the winner node (BMU) as the neuron, such that the distance between the input vector and the neuron is smallest.

- **Step 4:** Update the weights of the winner neuron and all its adjacent nodes:

$$w(t + 1) = w(t) + \theta(t) \times L(t) |V(t) - w(t)| \quad (6.2)$$

where  $L(t)$  is defined as the learning rate,  $\theta(t)$  is the neighborhood kernel function centered on the winner unit,  $w(t)$  is current weight of the neuron and  $w(t + 1)$  represents the updated weight. The amount by which the weights of an input vector is adjusted is determined by  $\theta(t)$  given by

Equation 6.3.

$$\theta(t) = \exp\left(-\frac{\text{dist}^2}{2\sigma^2(t)}\right) \quad t = 1, 2, 3, \dots \quad (6.3)$$

Where  $\text{dist}$  is the distance of a node from the BMU and  $\sigma$  is the width of the neighbourhood function as calculated by Equation 6.3.

- **Step 5:** Reduce the learning rate and the radius of the neighborhood. The exponential decay function for the neighborhood is given below:

$$\sigma = \sigma_0 \exp\left(\frac{-t}{\lambda}\right) \quad t = 1, 2, 3, \dots \quad (6.4)$$

where  $\sigma_0$ , indicates the width of the map at time  $t_0$ ,  $\lambda$  denotes a time constant and  $t$  is the current iteration. The learning rate is also reduced similarly.

- **Step 6:** Reiterate Steps (2)-(5) until the convergence condition is fulfilled.

In order to assign labels to SOM neurons we maintain a hit ratio between the neuron and the training set row. After a neuron is selected as a winning neuron it is tested against the training set to determine its class. If the neuron wins for larger number of attack samples as compared to normal data samples, it is classified as an attack, and as normal otherwise.

### 6.1.4 SOM Testing

Once the ordered SOM structure is obtained from the training phase, the testing is done as follows:

- **Step 1:** For each input vector compute the BMU based on the SOM map obtained from training phase.
- **Step 2:** Classify the incoming vector as:
  - Classify input vector as an normal if BMU is tagged as normal.
  - Classify input vector as an attack if BMU is tagged as attack.
- **Step 3:** Also determine the accuracy of SOM using the following parameters:
  - *True positive:* An incoming vector is identified as attack or normal and the BMU corresponds to this label respectively. For example an input vector is classified as an attack and the BMU is labeled as an attack.
  - *False Positive:* An incoming vector is identified as attack or normal but the BMU label does not confirm this. For example, an input vector is identified as normal but BMU is labeled as an attack.

## 6.2 Simulation Results

In the simulation tests, datasets modeled in Chapter 4 are used to determine the accuracy of our proposed approach to accurately classify smart grid data into

normal and anomalous. The testing of the SOM is conducted through the introduction of unlabelled data samples to the SOM, and observation of the class labels of the best matching nodes. The SOM is modeled as a rectangular matrix of varying sizes. Random initialization is used to assign weights to the neuron vectors. The training parameters selected for running the simulations are presented in Table 6.1.

Initial $L(t)$	0.5
SOM Map size (Variable)	$2 \times 2$ to $10 \times 10$
$L(t)$ decay function	Exponential
Training Iterations	75600
Neighborhood Function	Gaussian
Topology	Matrix

Table 6.1: SOM Training Parameters.

### 6.2.1 True Positives versus False Positives (Fixed Attack to Normal Ratio)

Figures 6.2 - 6.7 present a comparison of the true positives and the false positives generated through simulation, for the five varying dataset labels. It can be observed that varying the size of the SOM map has an effect on the detection rate. It can be concluded from the results obtained that the dataset where 45% of devices in a sample behave normally provides the best true positive rate and this rate is achieved for a map size of  $4 \times 4$ . Also it can be noted that for almost

all datasets the maximum true positives are reported for the  $4 \times 4$  map size. For a 25% ratio dataset, the highest detection rate was observed to be 57% at the cost of 49% false positives. For larger map sizes, the false positives were found to outweigh the detection rates. A similar trend was observed for the other datasets tested. For the 25%, 35%, and the 45% datasets, a common trend observed was of having the detection rate of a  $5 \times 5$  map outperforming other map sizes. However, for the 55% and 65% datasets, the trend did not continue, and a consistent detection rate of 40% was observed regardless of map size, for a constant set of false positives of 60% generated.

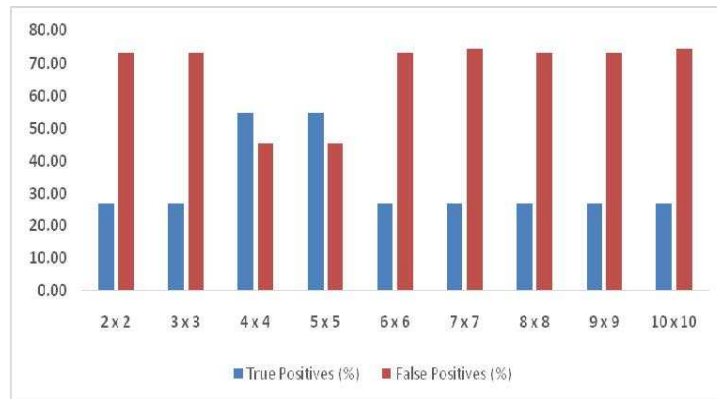


Figure 6.2: TP VS FP with 25% ratio dataset.

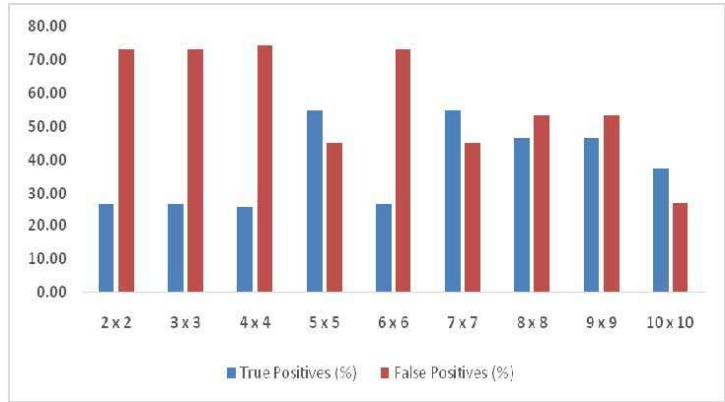


Figure 6.3: TP VS FP with 35% ratio dataset.

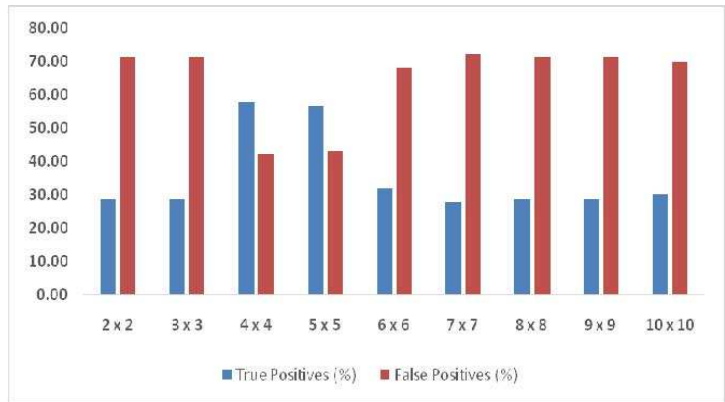


Figure 6.4: TP VS FP with 45% ratio dataset.

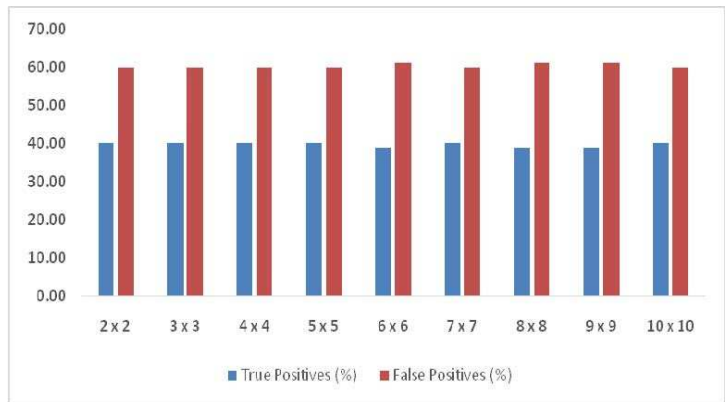


Figure 6.5: TP VS FP with 55% ratio dataset.

The true and false rates remain nearly constant from 55% dataset onwards. There is a slight decrease in the number of false positives and increase in the number of true positives for a 55% dataset when a  $10 \times 10$  map size is chosen.

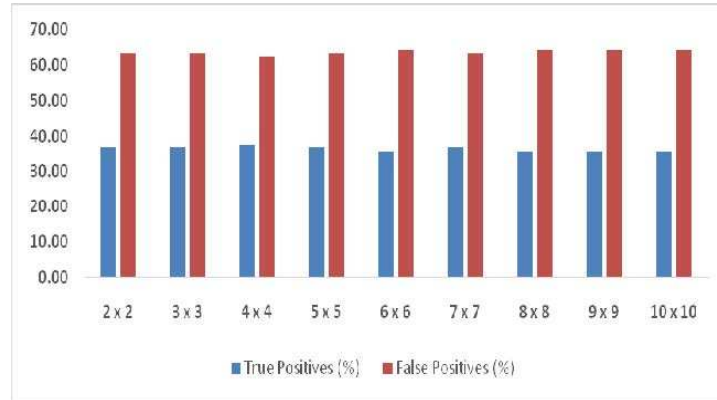


Figure 6.6: TP VS FP with 65% ratio dataset.

The comparison of the 65% dataset to the 55% reveals a much larger percentage of false positives for the 65% dataset. Also the true positives for the 65% dataset are smaller. However, again like the 55% dataset the two measured parameters remain constant for varying map sizes.



Figure 6.7: TP VS FP with 50% ratio dataset.

The two measured parameters remain identical for the 50% dataset.



## 6.2.2 Execution Time

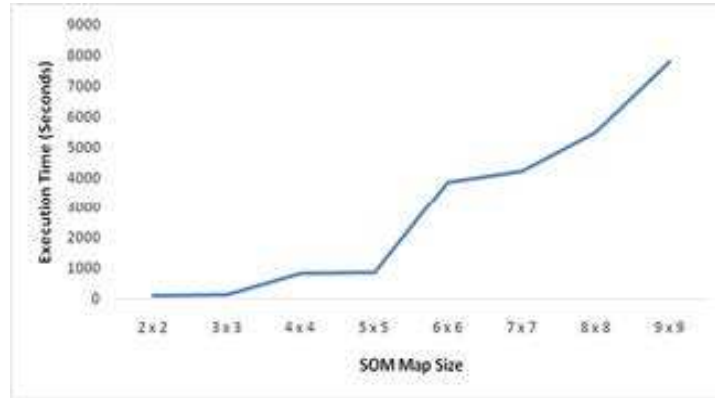


Figure 6.8: Execution time of SOM training for varying map sizes.

The size of the SOM has a direct impact on the delays incurred at time of training. In Figure 6.8, an illustration of the execution time for the SOM training for varying map sizes is provided. It can be inferred that for map sizes of  $5 \times 5$  and below, the training time is less than 1000 seconds, whereas, for larger map sizes, the time required to train the map for the same dataset is exceedingly high, with 9000 seconds being the peak value observed for a  $10 \times 10$  map.

In this chapter, we proposed a SOM-based data clustering approach towards classification of the modeled smart grid data into normal or anomalous. The proposed approach was subsequently tested for specific parameters and varying map sizes. From the results obtained, our proposed approach was found to provide reasonable accuracies of close to 60% when a map of size  $5 \times 5$  was selected, for two datasets. The overhead of the scheme was found to be relatively high for large map sizes, but within bounds ( $< 1000$  seconds) for smaller map sizes of  $5 \times 5$  and less.

# REFERENCES

- [1] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid - the new and improved power grid: A survey,” *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.
- [2] “Smart Grid 101: The Traditional Grid.” [Online]. Available: [http://www.smartgridnews.com/artman/publish/Business\\_Smart\\_Grid\\_101/The-Traditional-Grid-1599.html#.UNQ8-G\\_0DOs](http://www.smartgridnews.com/artman/publish/Business_Smart_Grid_101/The-Traditional-Grid-1599.html#.UNQ8-G_0DOs).
- [3] “Smart Grid Communications Overview,” 2012. [Online]. Available: [http://www.knowtex.com/nav/smart-grid-communications-overview\\_35327](http://www.knowtex.com/nav/smart-grid-communications-overview_35327).
- [4] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, “Smart grid technologies: Communication technologies and standards,” *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, Nov. 2011.
- [5] W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid.” *Computer Networks*, vol. 55, no. 15, pp. 3604–3629, 2011.

- [6] “Smart Grid Conceptual Model,” 2012. [Online]. Available: <http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model>.
- [7] “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,” *NIST Special Publication 1108*, 2010. [Online]. Available: [http://www.nist.gov/public\\_affairs/releases/upload/smartgrid\\_interoperability\\_final.pdf](http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf).
- [8] Y. Zhang, W. Sun, L. Wang, H. Wang, R. Green, and M. Alam, “A multi-level communication architecture of smart grid based on congestion aware wireless mesh network,” in *North American Power Symposium (NAPS), 2011*, Aug. 2011, pp. 1–6.
- [9] A. Shreyas, “Analysis of communication protocols for Neighborhood area Network for Smart Grid.” [Online]. Available: <http://hdl.handle.net/10211.9/849>.
- [10] M. Huq and S. Islam, “Home area network technology assessment for demand response in smart grid environment,” in *20th Australasian Universities Power Engineering Conference (AUPEC 2010)*, Dec. 2010, pp. 1–6.
- [11] E. Pallotti and F. Mangiatordi, “Smart grid cyber security requirements,” in *Proceedings of 2011 10th International Conference on Environment and Electrical Engineering, Rome, Italy*, 08 - 11 May 2011, pp. 1–4.
- [12] D. Zamboni, “Using internal sensors for computer intrusion detection,” Ph.D. dissertation, Purdue University, West Lafayette, Indiana, 2001.

- [13] “Common Types of Network Attacks.” [Online]. Available: <http://technet.microsoft.com/en-us/library/cc959354.aspx>.
- [14] H. Debar, “An introduction to intrusion-detection systems,” in *Proceedings of Connect*, 2002.
- [15] T. Lappas and K. Pelechrinis, “Data Mining Techniques for Network Intrusion Detection Systems,” *Department of Computer Science and Engineering, Riverside CA 92521*, 2007.
- [16] J. Caberera, B. Ravichandran, and R. Mehra, “Statistical traffic modeling for network intrusion detection,” in *8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2000)*, San Francisco, California, USA, Aug. 2000, pp. 466–473.
- [17] H. Wang, D. Zhang, and K. G. Shin, “Detecting syn flooding attacks,” in *Proceedings of the IEEE Infocom*, vol. 3, Jun. 2002, pp. 1530–1539.
- [18] A. Lakhina, M. Crovella, and C. Diot, “Diagnosing network-wide traffic anomalies,” in *Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*. Portland, Oregon, USA: ACM, 2004, pp. 219–230.
- [19] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, “The KDD process for extracting useful knowledge from volumes of data,” *Communications of the ACM*, vol. 39, no. 11, pp. 27–34, 1996.

- [20] I. Hendrickx, “Local classification and global estimation: Explorations of the  $k$ -nearest neighbor algorithm,” Ph.D. dissertation, Tilburg University, 2005.
- [21] W. W. Cohen, “Fast Effective Rule Induction,” in *Proceedings of the Twelfth International Conference on Machine Learning*. Tahoe City, California: Morgan Kaufmann, Jul. 1995, pp. 115–123.
- [22] S. M. Sait and H. Youssef, *Iterative computer algorithms with applications in engineering - solving combinatorial optimization problems*, 1st ed. Los Alamitos, CA, USA: IEEE Computer Society Press, 1999.
- [23] Z. Bankovic, S. Bojanic, and O. N. Taladriz, “Evaluating sequential combination of two genetic algorithm-based solutions for intrusion detection,” in *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems (CISIS 08)*. Genova, Italy: Springer, Oct. 2008, pp. 147–154.
- [24] A. Islam, A. Azad, K. Alarm, and S. Alam, “Security attack detection using genetic algorithm (ga) in policy based network,” in *International Conference on Information and Communication Technology (ICICT 2007)*, Dhaka, Bangladesh, Mar. 2007, pp. 341–347.
- [25] O. Folorunso, O. O. Akande, A. O. Ogunde, and O. R. Vincent, “Id-somga: A self organising migrating genetic algorithm-based solution for intrusion detection,” *Computer and Information Science*, vol. 3, no. 4, pp. 80–92, 2010.

- [26] W. Li, "Using genetic algorithm for network intrusion detection," in *Proceedings of the United States Department of Energy Cyber Security Group 2004 Training Conference*, 2004, pp. 24–27.
- [27] L. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338 – 353, 1965.
- [28] Y. Dhanalakshmi, "Intrusion detection using data mining along fuzzy logic and genetic algorithms," *International Journal of Computer Science and Network Security*, vol. 8, no. 2, pp. 27–32, 2008.
- [29] J. Gomez and D. Dasgupta, "Evolving fuzzy classifiers for intrusion detection," *Proceedings of the 2002 IEEE Workshop on Information Assurance*, Jun. 2001.
- [30] M. Saniee Abadeh, J. Habibi, Z. Barzegar, and M. Sergi, "A parallel genetic local search algorithm for intrusion detection in computer networks," *Engineering Applications of Artificial Intelligence*, vol. 20, no. 8, pp. 1058–1069, 2007.
- [31] A. K. Ghosh, A. Schwartzbard, and M. Schatz, "Learning program behavior profiles for intrusion detection," in *Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, California, 1999, pp. 51–62.
- [32] J. Ryan, M. J. Lin, and R. Miikkulainen, "Intrusion detection with neural networks," in *Advances in Neural Information Processing Systems*. Cambridge, MIT Press, 1998, pp. 943–949.

- [33] S. Mukkamala, G. Janoski, and A. Sung, "Intrusion detection using neural networks and support vector machines," in *Proceedings of the IEEE International Joint Conference on Neural Networks (ANNIE)*, vol. 2, Honolulu, USA, 2002, pp. 1702–1707.
- [34] E. Michailidis, S. Katsikas, and E. Georgopoulos, "Intrusion detection using evolutionary neural networks," in *Proceedings of the 2008 Panhellenic Conference on Informatics*, Washington, DC, USA, Aug. 2008, pp. 8–12.
- [35] J. Tian and H. Gu, "Anomaly detection combining one-class svms and particle swarm optimization algorithms." *Nonlinear Dynamics*, vol. 61, no. 1-2, pp. 303–310, 2010.
- [36] J. Ma, X. Liu, and S. Liu, "A new intrusion detection method based on bpso-svm," in *Proceedings of the 2008 International Symposium on Computational Intelligence and Design*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 473–477.
- [37] T. Verwoerd and R. Hunt, "Intrusion detection techniques and approaches," *Computer Communications*, vol. 25, no. 15, pp. 1356–1365, 2002.
- [38] S. A. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion detection using sequences of system calls," *Journal of Computer Security*, vol. 6, no. 3, pp. 151–180, Aug. 1998.
- [39] J. Kephart, "A biologically inspired immune system for computers." MIT Press, Jul. 1994, pp. 130–139.

- [40] P. L. Piotr and M. I. Heywood, “Dynamic intrusion detection using self-organizing maps,” 2002.
- [41] L. Lifen and Z. Changming, “Alert clustering using integrated som/pso,” in *International Conference on Computer Design and Applications (ICDDA 2010)*, vol. 2, Northeastern Univeristy, Qinhuangdao, China, Jun. 2010.
- [42] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber physical security of a smart grid infrastructure,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195 –209, Jan. 2012.
- [43] T. Baumeister, “Literature review on smart grid cyber security,” University of Hawaii, Honolulu, Hawaii, Tech. Rep., Dec. 2010.
- [44] A. Valdes and S. Cheung, “Intrusion monitoring in process control systems,” in *Proceedings of the 42<sup>nd</sup> Hawaii International Conference on System Sciences*, Big Island, Hawaii, Jan 2009.
- [45] Y. Jiaxi, M. Anjia, and G. Zhizhong, “Cyber security vulnerability assessment of power industry,” in *2006 IEEE Region 10 Conference (TENCON 2006)*, Wan Chai, Hong Kong, Nov. 2006, pp. 1 –4.
- [46] H. Li, R. Mao, L. Lai, and R. Qiu, “Compressed meter reading for delay-sensitive and secure load report in smart grid,” in *First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010)*, Gaithersburg, Maryland USA, Oct. 2010, pp. 114 –119.



- [47] A. Rial and G. Danezis, “Privacy-preserving smart metering,” in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society (WPES 2011)*, Chicago, Illinois, USA, 2011, pp. 49–60.
- [48] R. Berthier and W. H. Sanders, “Specification-based intrusion detection for advanced metering infrastructures,” in *Proceedings of the 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*. Washington, DC, USA: IEEE Computer Society, 2011, pp. 184–193.
- [49] D. Varodayan and G. Gao, “Redundant metering for integrity with information-theoretic confidentiality,” *IEEE SmartGridComm’10*, Oct. 2010.
- [50] R. Berthier, W. Sanders, and H. Khurana, “Intrusion detection for advanced metering infrastructures: Requirements and architectural directions,” in *First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010)*, Gaithersburg, Maryland USA, Oct. 2010, pp. 350–355.
- [51] L. Xie, Y. Mo, and B. Sinopoli, “False data injection attacks in electricity markets,” in *First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010)*, Gaithersburg, Maryland USA, Oct. 2010, pp. 226–231.
- [52] Z. Baig, “On the use of pattern matching for rapid anomaly detection in smart grid infrastructures,” in *IEEE International Conference on Smart Grid Communications (SmartGridComm 2011)*, Brussels, Belgium, Oct. 2011, pp. 214–219.

- [53] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, “Design principles for power grid cyber-infrastructure authentication protocols,” in *43rd Hawaii International Conference on System Sciences (HICSS 2010)*, Kauai, Hawaii, Jan. 2010, pp. 1–10.
- [54] J. Zhang and C. Gunter, “Application-aware secure multicast for power grid communications,” in *First IEEE International Conference on Smart Grid Communications (SmartGridComm 2010)*, Gaithersburg, Maryland USA, Oct. 2010, pp. 339–344.
- [55] B. M. Werners, “Aggregation models in mathematical programming,” in *Mathematical Models for Decision Support*. Berlin, Germany: Springer, 1988, pp. 295–305.
- [56] H. J. Zimmermann, *Fuzzy Set Theory and its Applications*, 4th ed. Springer, Oct. 2001.
- [57] P. Melin, “Signature recognition with a hybrid approach combining modular neural networks and fuzzy logic for response integration,” in *Modular Neural Networks and Type-2 Fuzzy Systems for Pattern Recognition*. Springer, 2012, vol. 389, pp. 77–92.
- [58] S. Barker, A. Mishra, D. Irwin, and E. Cecchet, “Smart\*: An Open Data Set and Tools for Enabling Research in Sustainable Homes,” 2012.
- [59] H. Xue, Q. Yang, and S. Chen, “Svm: Support vector machines,” in *The Top Ten Algorithms in Data Mining*, 2009, ch. 3, pp. 37–59.

- [60] V. N. Vapnik, *The nature of statistical learning theory*. New York, USA: Springer, 1995.
- [61] X. Haijun, P. Fang, W. Ling, and L. Hongwei, “Ad hoc-based feature selection and support vector machine classifier for intrusion detection,” in *IEEE International Conference on Grey Systems and Intelligent Services (GSIS 2007)*, Nanjing, China, Nov. 2007, pp. 1117–1121.
- [62] T. Joachims, “Making large-scale support vector machine learning practical,” in *Advances in Kernel Methods - Support Vector Learning*. Cambridge, USA: MIT Press, 1999, pp. 169–184.
- [63] X. Bao, T. Xu, and H. Hou, “Network intrusion detection based on support vector machine,” in *International Conference on Management and Service Science (MASS '09)*, Sep. 2009, pp. 1–4.
- [64] C. W. Hsu and C. J. Lin, “A comparison of methods for multiclass support vector machines,” *IEEE Transactions on Neural Networks*, vol. 13, no. 2, pp. 415–425, Mar. 2002.
- [65] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, “The weka data mining software: An update,” *SIGKDD Explorations*, vol. 11, no. 1, pp. 10–18, 2009.
- [66] R. Rojas, “Unsupervised Learning and Clustering Algorithms.” Springer, 1996.

- [67] T. Kohonen, *Self-organization and associative memory: 3rd edition*. Berlin: Springer, 1989.
- [68] “Kohonen’s Self Organizing Feature Maps.” [Online]. Available: <http://www.ai-junkie.com/ann/som/som1.html>.

# Vitae

- Name: Saif Ahmad
- Nationality: Indian
- Date of Birth: 05-04-1985
- Email: *sai598@gmail.com*
- Present Address: P.O. Box 598, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
- Permanent Address: 88/361, Humayun Bagh, Chamanganj, Kanpur 208001 (U.P.), India
- Tel (Res.): 966-3-8605449