DEEP LEARNING-BASED DETECTION OF ELECTRICITY THEFT CYBER ATTACKS IN SOLAR PV DISTRIBUTED GENERATION

A Thesis

by

MAHESH NAIDU

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Chair of Committee,	Erchin Serpedin
Co-Chair of Committee,	Khalid Qaraqe
Committee Members,	Katherine Davis
	Theodora Chaspari
Head of Department,	Mirsolav M. Begovic

August 2019

Major Subject: Electrical Engineering

ABSTRACT

In the past, electricity thefts were committed through physical means like tapping a line or bypassing the energy meter. However, the advent of smart meters has added another possible means of committing electricity theft that is through cyber-attacks. Existing research in this area focuses on detection of cyber-attacks that are aimed at reducing electricity bills by sending lower consumption readings to the utilities. This thesis describes artificial intelligence-based methods to identify cyber-attacks in Solar Photovoltaics (PV) distributed generation smart meters installed in houses that generate solar power for self-consumption as well as for sending excess power to the grid in exchange for incentives. In this work, we propose Deep Learning models: Feed Forward, Gated Recurrent Unit (GRU) and Convolutional Neural Network - Gated Recurrent Unit (CNN-GRU) to detect electricity theft cyber-attacks aimed at falsifying the generated energy readings for unlawful gains. A unique deep learning-based detector that trains on multiple datasets is also introduced herein thesis. It is found that such a detector presents a higher predictive performance. Hyperparametric-tuning of the models using cross-validated random-search for enhanced performance is also carried out in this thesis.

DEDICATION

I dedicate this research to my beloved parents who seamlessly supported me in my quest for higher learning and gave me valuable advice whenever I needed help in making important decisions.

To my teachers, mentors, friends, brothers, sisters and relatives whose good wishes, blessings and words of encouragement have helped me finish this study.

And finally, I dedicate this research to the Almighty God, for giving me good health, strength and perseverance that were much needed throughout this journey.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to Dr. Erchin Serpedin, Advisor, and Dr. Muhammad Ismail, PhD Mentor, for their support and guidance throughout my master's program. They have always supported me and taught me how to be productive and successful. I wholeheartedly appreciate the freedom they gave me to do my research. I am thankful for their insightful coaching, tremendous support and encouragement.

I would like to express my sincere thanks to Dr. Khaliq Qaraqe, Co-Advisor, Dr. Katherine Davis and Dr. Theodora Chaspari for graciously agreeing to serve on my Thesis Committee.

I would also like to thank Dr. Mostafa Shaaban for mentoring and helping me at various stages of my research by providing crucial data and information.

It has been a great pleasure working with the faculty, staff, and friends at Texas A&M University, during my journey through the master's program. I appreciate the Electrical and Computer Engineering Department and College of Engineering for their logistic support through the program.

Finally, I would like to thank my family and friends for their encouragement and invaluable support throughout my education. I thank my family for believing in me.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supported by a thesis committee consisting of Dr. Erchin Serpedin [advisor], Dr. Khalid Qaraqe and Dr. Katherine Davis of the Department of Electrical and Computer Engineering and Dr. Theodora Chaspari of the Department of Computer Science and Engineering.

All work for the thesis was completed by the student, under the advisement of Dr. Muhammad Ismail of the Department of Electrical and Computer Engineering.

Funding Resources

There are no outside funding contributions to acknowledge related to the research and compilation of this document.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

CHAPTER I

INTRODUCTION

I.1 Motivation

The Power and Energy Sector has always been an integral part of a nation's economy and plays an important role in shaping its future. The expansion of the Power Grid infrastructure is today a crucial component of a nation's development and growth model. This is because all economic activities require energy, whether to run machines and appliances, electrify homes and offices, provide transportation, or manufacture goods. However, a pressing problem that this sector faces is electricity theft. Electricity theft is known to have brought enormous losses to utility companies around the world, both in terms of power and revenue. In the African continent, many countries lose a significant portion of electricity to theft itself. South Africa alone is facing six forms of electricity theft resulting in an average loss of 1.5 billion dollars per annum [1]. According to local reports, bypassing of electricity meters and illegal connectivity to the grid are the two most common ways of committing electricity theft. In India, after transmission and distribution (T&D) losses, a major chunk of energy is lost to electricity theft. According to a World Bank data, power theft reduces India's GDP by over 1.5%. Therefore, electricity theft is a grave problem that needs to be tackled not only by good policy-making but also by developing technologies that can help detect its presence and mitigate its effects.

I.2 Commercial Losses in Electric Power Systems

Commercial losses attributed to electricity theft are referred to as non-technical losses (NTL), and the other kind is referred to as technical losses (TL). Non-technical losses affect quality of supply, increase load on the generating station, and affect the tariff imposed on honest

customers. Technical losses are the losses inherent to the operations of an electrical network and occur as power flows through equipment such as cables, overhead lines and transformers. The two kinds of electric power losses will be briefly described in the following sections.

I.2.1 Technical Losses

Technical losses occur when power is dissipated by equipment and conductors during the transmission and distribution stages. In fact, losses accompany the generated power right from the beginning, i.e., the generation phase. The power generated in power stations passes through large and complex networks like transformers, overhead lines, cables and other equipment and then reaches the end users. The difference between the generated and distributed power is called transmission and distribution loss. A major component of this loss occurs over the transmission lines also referred to as line loss. Hence, to reduce this excess loss, the generated power is stepped-up to a very high voltage (11 kV/ 33 kV) and then transmitted via the transmission lines. This is followed by a step-down procedure to bring the voltage to a lower ready-to-use value. A higher voltage across transmission lines causes a drop in the current which in turn reduces the ohmic loss or copper loss (I^2R) associated with the conductors. The other losses that form the technical losses are corona loss, leakage current loss, dielectric loss, etc. Ideally, technical losses should not exceed beyond 20% of the generated power; however, in many countries it accounts for over 23% to 25% of the generated power.

I.2.2 Non-Technical Losses – Electricity Thefts

Non-technical losses are mainly attributed to electricity thefts. Electricity thefts are committed using many different methods. The most common yet dangerous method is tapping the electricity from a distribution line. This method carries deadly risks. Many offenders pay for the power they steal with their lives. Besides, stealing electricity by this method overloads the

system which often causes the power connection to trip or fail and can also cause fire. The second most prominent way of power theft is through the meter which records electricity consumption. The meter could be compromised in many ways:

- Bypassing the energy meter: In this method [2], the input and output terminal of the energy meter are short-circuited, preventing the consumption from registering in the meter.
- A strong magnet is sometimes placed very close to electromagnetic meters slowing down its rotating disc. A slow rotating disk records less energy consumption.
- Strong magnetic fields could also be used to wipe out the memory in meters.
- Neutral current reverse method: In this method, the neutral is externally grounded, and the meter is externally grounded, so voltage cannot be measured and hence the phase angle cannot be measured. So, the power cannot be determined, and the meter does not show any power utilized.
- Resetting the meter reading.
- Damaging the pressure coil of the meter.
- Physically impacting the meter

Non-technical losses, caused mainly due to electricity theft, adversely affect all entities such as power plants, utilities and customers that are part of the electric power network. In the reference [3], the effect of electricity theft on the quality of power supply has been explained in detail. It talks about how electricity theft leads to steady state voltage drop across the distribution buses which in turn results in the poor quality of power supply. This reference describes the desirable voltage range to be from 202 V to 231 V for rated voltage of 220 V and from 117 V to 133 V for rated voltage of 110 V. Without electricity theft while also considering technical losses (TL), the voltage on the system buses remains within the ideal steady state voltage limits.

However, with addition of load due to electricity theft, the voltage on the bus bars enters the undesirable range which is indicative of a poor power supply quality. The work [4] gives an overview of the effects of electricity theft on utilities and consumers. Power theft adds additional unaccounted load on the system about which the utilities have no estimates. Hence, it becomes unclear as to how much power needs to be supplied from the generation unit. This causes the generation unit to trip affecting the power supply to all customers. Besides, electricity theft is not a victimless crime as it ultimately increases the cost of electricity to every paying customer. In the energy sector, the utility companies earn revenue from the supply of power and the service they offer to the customers. But, a considerable portion of this revenue is lost due to the NTL losses. Hence, to protect themselves from running into losses, utilities are forced to increase the tariff on electricity. This burdens honest customers with higher electricity bills.

The adverse effects of electricity-theft discussed above clearly indicate that power theft is a serious problem with significant economic implications. With this view and in perspective, extensive research is being conducted in the area of electricity theft detection. More information about the research work done in this area can be found in the literature review section. However, it is observed that the focus of research in this area has always been on theft in power consumption where the objective basically is to reduce electricity bills. In this thesis, the critical problem of power theft is being dealt with but in the scenario of energy generation. Novel state-of-the-art detection mechanisms based on Neural Networks have been devised to detect electricity thefts in a Distributed Generation System. Distributed Generation System is an integrated system that enables local units to become self-sufficient in power as well as become contributors of power for the benefit of all. It allows local units to have power generating installations for self-consumption. Besides, it also offers them the opportunity to sell the excess

power to the utilities. More discussions on Distributed Generation will be presented in the coming sections. Like in case of consumption, smart meters are employed to report generated power readings to the utilities accurately and efficiently. Being smart devices, these might be hacked by malicious agents to report false readings to the utility companies for illegal gains. The aim of this research is to detect such cyber-attacks by understanding the patterns in data transmitted by these meters.

I.3 Electricity Theft in AMI Networks

I.3.1 AMI Networks

Advanced metering infrastructure (AMI) is an architecture for automated, two-way communication between a smart utility meter and the utility company [5]. It is an integrated system of smart meters, communication networks and data-management systems. The installation of advanced metering infrastructure networks has facilitated the adoption of smart meters around the world. This has made reporting and communication of metering information much easier as the data is now transmitted over wireless channels. The AMI system also presents other unique features and services to offer. Not only does it provide utility companies with real-time data about power consumption but also allows customers to make informed decisions about energy usage. Combined with appliances like in-home displays and communicating thermostats, AMI offers customers time-based pricing programs and incentives that encourage customers to reduce peak demand and manage costs and consumption. Equally significant is its contribution towards outage management and service restoration. The report [6] issued by the Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, lists out the benefits from the 70 SGIG (Smart Grid Investment Grants) projects implementing AMI and also gives insights on theft detection. The key findings in this report indicate that Operations and

Maintenance (O&M) cost savings from remote metering services for e.g., remote billing is the major benefit of AMI networks. Remote meter reading does away with the need of manually taking down meter readings and helps generate more timely and accurate bills. Besides generating bills, many customer complaints and concerns are addressed remotely, which improves customer service and satisfaction. Additionally, the report talks about electricity theft in AMI and the importance of cyber security in smart meters which is the focus of this research. It also talks about AMIs being used today in conjunction with the Meter Data Management system (MDMS) to detect electricity theft. Many utilities have systems that issue alarms when irregularities in consumption activity are identified. However, these irregularities are not always due to electricity theft. Hence, apart from hardware and software solutions, utilities are now working to develop better data analytics to differentiate actual theft incidents from the many different events that can trigger alarms. Data analytics can be utilized to reduce the number of such false alarms. This thesis focuses on how to leverage patterns in data to accurately predict electricity thefts with minimum false alarms or false positives.

I.3.2 Electricity Theft Cyber Attacks

Smart meters are not safe from hackers. Several security and privacy issues arise in deploying the smart grids, especially because of wireless communications [7]. For instance, wireless communications can be intercepted by malicious observers if the data exchanged is plaintext and lacks proper encryption. Sensitive information like personal data or energy usage pattern of customers could be extracted by observers along the network exposing the customers to privacy invasion.

This research lays emphasis on electricity theft cyber-attacks in utility smart meters and its implications. Wireless communications provide the opportunity to carry out electricity theft

without physically tampering with the meter. Such attempts may easily go unnoticed by utilities; thus, further adding to the already high non -technical losses. Once compromised, these devices could be programmed/ configured to transmit lower energy readings than actual in order to get reduced bills. However, in case of energy generation, smart meters could be programmed to amplify energy values for unlawful gains. This research is aimed at understanding cyber-attacks in Distributed PV Generation smart meters and finding novel ways to efficiently detect those attacks.

Noteworthy research has been conducted in electricity theft detection in power consumption. Recently, machine learning techniques were employed to detect electricity thefts. Chapter 3 discusses in detail, machine learning and deep learning-based detection of electricity theft cyber-attacks in AMI networks monitoring power consumption.

CHAPTER II

ELECTRICITY THEFT IN DISTRIBUTED PV GENERATION

II.1 Distributed Generation

Distributed generation (DG) is an approach that employs small-scale technologies to produce electricity close to the end users of power. As illustrated in Figure 1, DG technologies consist of renewable energy generators. They offer a number of potential benefits. They can provide lower-cost electricity and higher power reliability and security with fewer environmental consequences relative to traditional power generators. In the present scenario, electricity generation and distribution in the United States is dominated by centralized power plants. The power in these plants is typically due to combustion (coal, oil, and natural) or nuclear generated. Although, a significant portion of today's commercial energy requirement is met by centralized power plants, this system has its own set of disadvantages. In addition to power loss over lengthy transmission lines, these systems contribute to greenhouse gas emission, the production of nuclear waste, inefficiencies due to long distance transmission, environmental problems at the sites where the power lines are manufactured and deployed, and security related issues. These problems can be avoided by the adoption of a distributed generation system. Distributed generation is often implemented via small units like solar panels. These units can be standalone or integrated into the existing energy grids. Consumers who have installed solar panels can utilize the generated electricity and transfer the surplus power to the utilities for remuneration or incentives. In this way, they will contribute more to the grid than they can take out resulting in a win-win situation for both the power grid and the end-user. Currently, we have distributed generators owned by customers and they can sell electricity to the utility for financial gains.

However, malicious customers can manipulate the readings from their DG units in order to fool the utility with falsely higher generation power that is sold to the utility to achieve financial gain. The aim of this research is to identify such DG units that transmit malicious data to the utilities.

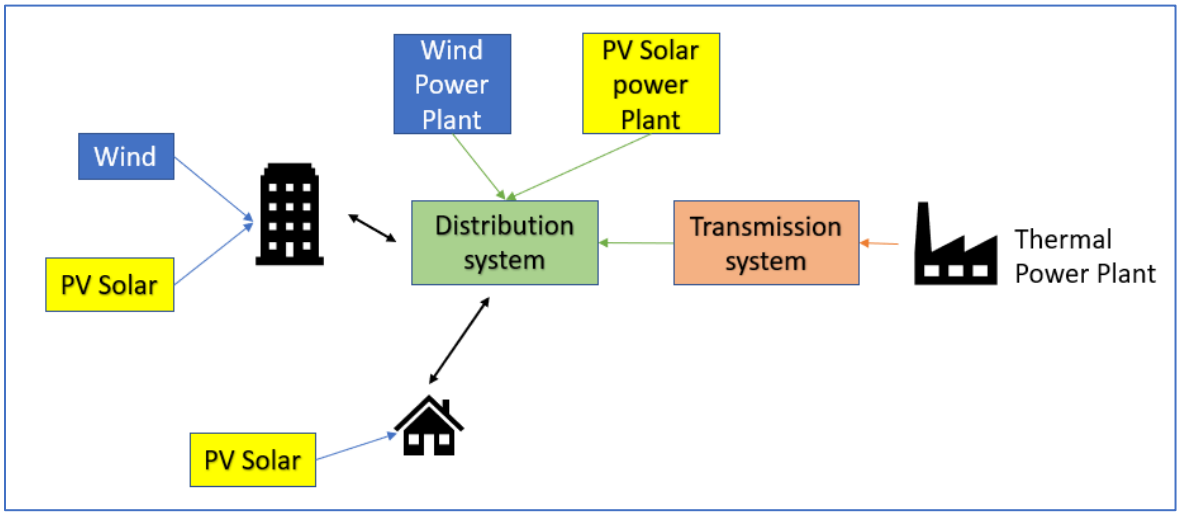

Figure 1. A distributed generation system

II.2 Cyber Attacks in Distributed Generation Smart Meters

Like smart meters monitoring power consumption, distribution generation smart meters can also be compromised with the intent of making illegal gains. These compromised smart meters can be programmed to report amplified generation readings to the utilities for unlawful financial gains. As mentioned before, Solar PV distributed generation can include both standalone or integrated DG units. Customers with standalone DG units will use them as auxiliary power supply units to supplement their energy demands which, for most part, are met by the grid supply. On the other hand, customers with integrated DG units will consume as well as supply excess power to the utilities in return for incentives. The latter is a true realization of a Distributed Generation system as it brings distantly located power stations and local generating units (DG units), which are also the end users, under one roof. Hence, an efficient detector is

required that trains on valid data that considers all aspects of Solar PV Distributed generation to identify electricity theft.

II.3 Problem Statement

In this thesis, novel deep learning techniques have been used to detect electricity theft cyber-attacks in Distributed PV generation. No existing literature talks about electricity theft in power generation. In this work the neural networks: Feed Forward, Gated Recurrent Unit (GRU) and Convolutional Gated Recurrent Unit (CNN-GRU) are proposed for creating the detectors. A unique deep learning-based detector that trains on multiple datasets simultaneously is also proposed. Such a detector is said to offer a higher predictive performance. Subsequently, the performance of the detectors is analyzed and the one that offers the best Detection rate and False Alarm rate is identified. The datasets have been prepared using irradiance measurements and practical PV panel data.

Also, the proposed detector is a generalized detector, i.e., it is trained to detect electricity theft cyber-attacks for all the customers of a utility. Hence, the detector is modeled on datasets pertaining to all the customers rather than a single customer. Only customer specific detectors would require datasets of single customers. There are two reasons behind going for a general detector rather than a single customer specific detector. Firstly, a general detector can cover new connections or new customers who would not have any historical data to share. Secondly, for training customer specific detectors, a customer might send false generation data to the utilities. A general detector overcomes both these issues. In the second case, even if a customer manages to send false data to the utility, the data might not significantly affect the performance of the detector as it has already been trained on a very large dataset.

In this thesis, we have assumed that the consumer units are DG units integrated with the power grid. The energy generated is immediately consumed and there are no storage cells available with the customers. The excess power is sent to the grid for which the customer is paid by the utilities.

II.4 Contributions

1. To model an unbiased detector, which trains on a dataset containing equal proportion of honest and malicious profiles, we devised a set of attack functions which will manipulate honest data in a manner that reflects possible actual ways of misrepresenting the generated energy data.
2. We propose the following deep learning-based models to detect electricity theft cyber-attacks: Deep Feed Forward, Gated Recurrent Unit (GRU) and Convolutional Gated Recurrent Unit (CNN-GRU) neural networks. These networks were trained, tested and validated on honest and malicious smart meter data.
3. We performed Hyperparametric Optimization (HPO) using Random Search (a parameter optimizing technique) to enhance the detector's performance. Depending on the type of data and the neural network model, hyperparametric optimization needs to be carried out to find the model's optimal hyperparameters that help in getting a better predictive performance.
4. We simulated the IEEE 123-bus test system to generate honest and malicious data sets for the DG units using practical load and irradiance data of a certain year with readings obtained every 60 minutes. More information about the datasets will be presented in the next sections. The honest and malicious datasets were then modeled with the Feed Forward (FF), Gated Recurrent Unit (GRU) and Convolutional Gated Recurrent Unit (CNN-GRU) neural networks to produce classifiers that can classify meter data readings as honest or malicious.

5. A unique deep learning-based detector is proposed that combines honest and malicious PV generation data with irradiance data to capture the correlation between these data streams. This approach is known to yield a better detection performance.

CHAPTER III

LITERATURE REVIEW AND RELATED WORK

In the past, several solutions and approaches were proposed to detect electricity theft cyber-attacks in the power consumption area. Some approaches are based on game theory [8] – [10], while another approach used computations involving entropy [11]. In [12], a pattern recognition approach based on optimum path forest was used and found to yield an accuracy of 89% for power theft detection. Another technique [13] was proposed, which involves a two-stage detector based on C-means fuzzy clustering and fuzzy classification and achieves an accuracy of 83% in terms of detection.

Data driven solutions have been more popular because of the vast streams of data that are obtained from utility smart meters. Many of these works use commonly used data-driven machine learning techniques that classify data into different classes like honest, malicious, etc. For instance, in [14], an electricity theft detector has been designed using a Support Vector Machine (SVM), which is a commonly used machine learning algorithm. In this work, historical consumption data of customers containing honest and fraudulent cases was first cleaned and pre-processed using data-mining techniques. Thereafter, feature selection and extraction were performed that resulted in 24 features representing 24 daily average kilowatt- hour consumption values of the customers. These 24 values, referred to as the load profiles of the customers, were then fed into the SVM based model for training and an accuracy of 86.43% was achieved for this electricity theft detector. This approach used SVM to classify honest and fraud cases by correlating abnormal patterns in data corresponding to electricity theft. Besides, this work used feature selection to obtain daily load profile of each customer. This was not exclusively needed in this thesis because the original data contained hourly kilowatt values recorded for (365 x 24)

hours for all the customers. In another research work in this area [15], decision trees (DT) were used along with SVM in a two-step approach. Herein work, the data processed by the decision tree is given as an input to the SVM for classification of honest and malicious data. The decision tree model is created based on input variables representing household attributes like number of appliances, number of members, etc., to predict the energy consumption. Subsequently, the predicted energy consumption along with the actual energy consumption and other customer features is fed to the SVM classifier. The SVM classifier then classifies the observations as malicious or honest based on the target label. An accuracy of 92.5 percent is achieved by this classification scheme. This work essentially adds another feature (predicted energy consumption) to the set of features that model the classifier. As a result, an improved detection performance is achieved, however, the paper could not explain how the addition of the feature – predicted energy consumption produces a strong correlation between the features.

Ideally, the accuracy of detection in the case of power-thefts should be high because many fraudulent cases may go undetected and also the probability of getting false alarms will be high. The aforementioned works use shallow machine learning techniques like SVM [14], [15] and thus cannot really capture the different patterns observed in complex data such as power metering data. This might result into detectors having low efficiency and accuracy. In such a scenario, deep learning holds a better promise as it is able to learn efficiently from the massive amounts of data provided by smart meters. In the paper [16], deep learning techniques are employed to determine the behavior features of FDI (False Data Injection) attacks in historical measurements data. The captured features are then utilized to detect the FDI attacks in real-time. Through feature selection, the devised model reduces the dependence on potential attack scenarios and achieves high accuracy. Often, the data obtained from smart meters exhibits a

time-series/sequential relationship. Traditional machine learning techniques cannot really exploit the information contained in this temporal correlation. In the reference [17], the time series nature of power consumption readings has been utilized using feedforward neural networks. The hourly consumption data of a household over a fixed period is used to train Deep Neural Networks for predicting the next/future value in the sequence which is already known. Thereafter, the root mean square (RMS) error between the actual value and the predicted value is observed. If the RMS error values for successive predictions go beyond a permissible limit, an alarm is raised, and the smart meter is adjudged malicious.

To model an unbiased detector, one must have a balanced dataset containing equal proportion of both honest and malicious data. The procurement of honest metering data can be managed; however, malicious data may not be easily available. To generate malicious data, one way is to create functions that manipulate honest meter readings by taking honest data as input and giving malicious data as output. This malicious data will represent a set of possible ways of manipulating honest data to carry out electricity-thefts. Previous works [18], [19] used a set of such functions called attack functions to generate malicious data. This malicious data was used to train Deep Neural Networks (DNNs) and Gated Recurrent Units (GRUs) against honest data. The proposed DNN and GRU based detectors in the aforementioned works achieved detection rates of 94% and 93%, respectively, and false alarm rates as low as 2.3% and 5%, respectively.

CHAPTER IV

DATA PREPARATION AND MODELING

IV.1 Honest Energy Generation Data

The IEEE 123-bus test system was used to generate the modeling datasets. Figure 2 depicts the IEEE 123-bus test feeder with inter-connected buses connected at different phases. The net power consumed/ produced by a bus in a phase is the sum of all the power that flows into/out of the bus in that phase. For instance, the consumption at bus 2 Phase c can be obtained by calculating the sum of the power flows from buses 1, 4 and 8 at phase c.

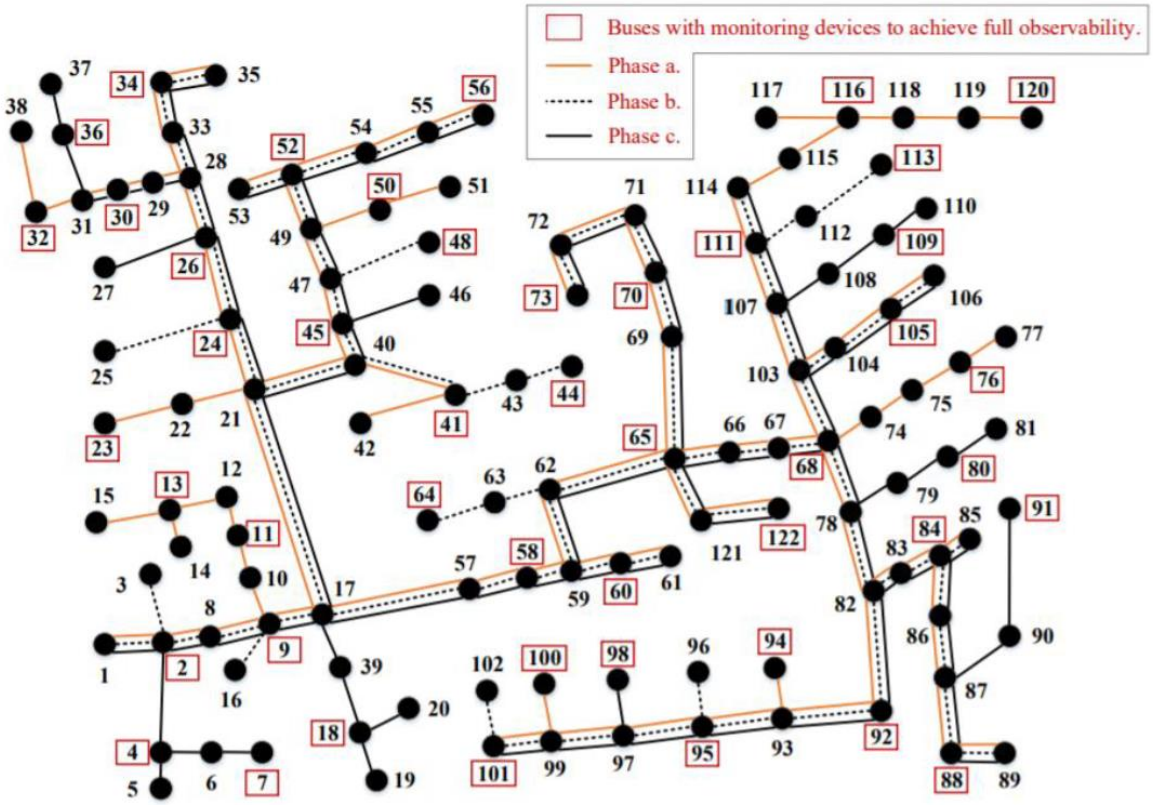

Figure 2. IEEE 123-bus system [21]

The active power demand (in kW) on the 122 buses and 3 phases of an actual IEEE 123-bus test feeder system was utilized to obtain the number of residential units connected to them. The active power demand on each phase of the buses was divided by 5 kW in order to obtain the number of residential units connected to it. This was done based on an assumption that the electrical load of a house is approximately 5 kW. The said computation resulted in a total of 514 residential customers, 200 in phase 1, 151 in phase 2 and 163 in phase 3. Table 1 shows the number of residential customers connected to the buses. All the residential customers are found between buses 51 and 122. The Buses 0 to 50 are for non- residential customers. The fields with the value '0' indicate no connected load.

Buses	Phase1	Phase2	Phase3		Buses	Phase1	Phase2	Phase3
51	4	0	0		87	0	0	0
52	7	7	7		88	8	0	0
53	14	14	14		89	0	0	4
54	7	14	7		90	0	0	4
55	0	0	8		91	0	0	8
56	4	0	0		92	0	4	0
57	8	0	0		93	0	8	0
58	8	0	0		94	8	0	0
59	0	0	0		95	0	0	0
60	4	0	0		96	0	8	0
61	0	4	0		97	0	0	0
62	0	0	0		98	0	0	8
63	0	4	0		99	0	0	0
64	0	4	0		100	8	0	0
65	4	0	0		101	0	4	0
66	4	0	0		102	0	4	0
67	0	0	0		103	0	0	0
68	0	0	0		104	8	0	0
69	0	0	8		105	0	8	0
70	8	0	0		106	0	0	8

Table 1. Connections of residential customers in IEEE 123-bus system

Buses	Phase1	Phase2	Phase3		Buses	Phase1	Phase2	Phase3
71	0	15	0		107	0	0	0
72	7	7	14		108	0	0	4
73	0	0	15		109	0	0	8
74	4	0	0		110	0	0	8
75	8	0	0		111	0	0	0
76	4	0	0		112	0	8	0
77	8	0	0		113	0	8	0
78	0	0	0		114	0	0	0
79	0	0	8		115	8	0	0
80	0	0	8		116	0	0	0
81	0	0	8		117	4	0	0
82	21	14	14		118	4	0	0
83	0	8	0		119	8	0	0
84	0	0	0		120	8	0	0
85	8	0	0		121	4	0	0
86	0	8	0		122	0	0	0

Table 1. Continued

IV.1.1 Preparation of Honest Energy Generation Data

The generated energy data of the above households was calculated/ simulated using the Random functions in MATLAB and the result was commensurate with practical generation profiles. Below are the steps involved in the preparation of Honest Energy Generation data:

- The *Irradiance data* containing solar irradiance readings (in W) recorded at intervals of 60 minutes for a year was used to simulate the generated energy data of the households. A total of 8760 readings for 8760 (365 x 24) hours were observed. Table 2 shows the irradiance profile for the first 11 days of a year.

Days	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23	T24
1	0	0	0	0	0	0	0	0	3.8	10.1	17	21.1	21.6	20.7	16	9.6	3.3	0.1	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	9.5	23.5	28.6	27	26.2	20.7	18.3	14	8.3	0.3	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	7	14.6	11.9	17.4	21.8	20.1	14.2	7.5	2.5	0.1	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	1.6	8.8	18.9	23.6	28.2	27.2	17.6	12	4	0.2	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0.1	1.6	8.7	20	32.1	47.5	33.3	18.1	10	3.6	0.4	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	3.4	13.2	22.2	24.8	35.4	40.7	35.6	22	9.2	0.3	0	0	0	0	0	0
7	0	0	0	0	0	0.1	0	0.1	3.1	11.1	15.9	21.4	30	26.1	19.2	13	4.1	0.2	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	2.4	10.4	23.4	30.8	35.8	42.4	36.6	24	9.3	0.4	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	7.2	24	37.7	45.3	44.5	44.8	37.7	26	11.3	0.6	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	4.6	18.2	32	42.3	47.4	45.9	37.6	24	9.9	0.6	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	4.5	18.1	30.8	40.7	43.3	40.4	26.7	22	10.1	0.4	0	0	0	0	0	0
365 rows																								

Table 2. Daily Irradiance profile recorded per hour (in W)

- 5 types of PV panels were chosen for this research and each household was assigned one type of panel. The assignment of panels to the households was done using the Random function in MATLAB. However, the number of panels of a particular type installed in each house depends on the PV capacity of that household. The PV Capacity of each household was randomly chosen between 0.5 kW and 1.5 kW. This range was decided based on information regarding standard installations. The characteristic parameters of each panel type can be found in Table 3.

Panel type	1	2	3	4	5
V_MPP (in V)	72.9	30.2	49.2	40.2	47
I_MPP	5.97	8.11	1.78	6	2.88
V_OC	85.6	37.8	61	50.7	61.3
I_SC	6.43	8.63	1.98	6.7	3.41
K_v	-0.0027	-0.0033	-0.0027	-0.003	-0.003
K_i	0.05	0.06	0.04	0	0.07
NOCT	45	46	45	47	45
PV_capacity(in kW)	0.435	0.245	0.0875	0.23	0.135

Table 3. Parametric information of 5 PV panel types

V_MPP is the 'Maximum Power Point Voltage' and it is the voltage at which PV module can produce maximum power. Similarly, I_MPP is the current at which a PV module can

produce maximum power. VOC or 'Voltage at Maximum Power' is the voltage that occurs when the module is connected to a load and is operating at its peak performance under standard test conditions (STC). Similarly, IOC is the corresponding current. NOCT stands for Nominal Operating Cell Temperature. It is the temperature reached by solar cells under standard conditions.

- These parameters specific to each panel type are combined with the *hourly irradiance data* (recorded per hour for a period of 1 year) to compute the solar power generated per hour per panel for each of the above panel types in one year. Table 4 shows the power generated by each panel type for the first 24 hours out of the 8760 hours (1 year) for which the data was generated.

Panel Type	1	2	3	4	5
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
8	0	0	0	0	0
9	17.87638	10.22595	3.61099	10.19831	5.573812
10	47.33172	27.05009	9.558958	26.95064	14.75685
11	79.33119	45.29048	16.0179	45.076	24.73135
12	98.21561	56.03646	19.82827	55.736	30.61685
13	100.512	57.34221	20.29154	57.03038	31.33248
14	96.37749	54.99111	19.45743	54.69962	30.04402
15	74.71054	42.65903	15.08542	42.46355	23.29117
16	45.0023	25.72075	9.088662	25.62817	14.03067
17	15.52893	8.883782	3.136861	8.860457	4.841911
18	0.471486	0.269855	0.095251	0.26928	0.147014
19	0	0	0	0	0

Table 4. Energy generated per hour by each panel

Panel Type	1	2	3	4	5
20	0	0	0	0	0
21	0	0	0	0	0
22	0	0	0	0	0
23	0	0	0	0	0
24	0	0	0	0	0

Table 4 Continued

Note that zero values are attributed to the hours when there was no generation. These hours are basically the ones for which there was no irradiance or sunlight.

- As mentioned before, the PV capacity (in kW) of each household shall be in the range 0.5kW and 1.5 kW. Each household unit will install PV panels of a single type out of the 5 types discussed before. Therefore, the number of PV panels allocated to each house can be calculated by dividing the household PV capacity with the PV capacity of each panel. PV Capacity of each panel can be obtained from Table 3.

$$\textit{No. of PV Panels} = \textit{Installed PV Capacity} / \textit{PV Capacity of each Panel}$$

- Once, the number of PV panels installed in each household is calculated, the yearly generation profile of a household can be obtained by multiplying the number of PV panels with the yearly generation profile of the installed panel-type provided in Table 4.

$$\textit{Generation profile of a house (year)} = \textit{No. of PV Panels} \times \textit{Generation profile of a panel (year)}$$

- By combining the generation profiles of all households (514), we get the *PV generation profile* of all households. The size of this dataset is 8760 × 514. The rows attribute to

readings taken in 1-hour interval for 8760 hours of a year whereas the columns represent the household numbers (514 in total).

These readings are recorded and transmitted by the smart meters of the individual DG units to the utilities for the purpose of billing and analysis. Since, the only way the utilities can obtain the generated power readings is through smart meters, there is a possibility that the smart meters could be compromised through cyber-attacks to send false readings to the utilities.

IV.2 Malicious Data

Distributed PV generation smart meter data transmitted to the utility is the key to deciding the remuneration being offered to the customers. The information sent by the DG unit smart meters is the only source of information that could be used to determine the amount of solar power generated and the remuneration to be offered to the customers. However, it is possible that malicious customers would tamper with the smart meter and send amplified generated power readings to the utilities. These amplified readings are malicious readings and the focus of this research is to identify such malicious readings.

To create an unbiased detector, we required equal proportion of both honest and malicious data. Lack of malicious data for training may not provide us with an efficient detector. This motivated us to prepare the malicious data by creating certain functions that will manipulate the honest PV generation profile and generate a malicious profile for the households. These functions are referred to as attack functions. In the context of this research, the PV generation profile represents the honest customer smart meter data. This data will be fed to the attack functions to generate malicious data that will be used along with honest data to train the detectors.

The PV generation profile obtained for each household is originally an array A of size 8760 × 1 where each successive value is the hourly generated power recorded over a period of one year (8760 hours). This profile is reorganized/reshaped to yield a daily profile of the households over a period of 24 hours. This results in a matrix of size 365 x 24 (see Table 5). Each row in this matrix represents the daily generated energy profile of a household (DG unit).

Days	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23	T24
1	0	0	0	0	0	0	0	0	54	142	238	295	302	289	224	135	47	1	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	134	329	399	377	366	290	257	193	117	4	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	94	194	159	231	289	267	189	100	34	1	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	22	119	254	316	376	363	237	158	54	3	0	0	0	0	0	0
5	0	0	0	0	0	0	0	1	22	117	268	426	624	442	243	139	49	5	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	47	182	304	339	481	551	484	295	127	4	0	0	0	0	0	0
7	0	0	0	0	0	1	1	1	42	149	213	285	398	347	256	169	55	3	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	34	146	325	426	494	582	505	328	130	6	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	102	338	526	629	618	622	526	369	160	9	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	63	248	432	567	633	614	505	328	135	8	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	63	250	422	554	588	550	366	299	140	6	0	0	0	0	0	0
	365 rows																							

Table 5. Daily generation profile of a household (in Wh)

From the above table, it can be observed that the time is split into a set of periods $T = \{1, \ldots, T\}$ with equal duration. The periods T cover the 24 hours of the day. The energy generation profile for each customer covers a set of days $D = \{1,...,D\}$. The value of D here is 365. Let the matrix in the above table, representing the actual energy generation values for a specific customer, be referred to as E where the rows represent days in D and columns represent the time periods in T. Let us denote the reported energy generation value by the customer to the utility company at time t and day d by $R(d, t)$. An honest customer reports the actual energy generation value, and hence, $R(d, t) = E(d, t)$. On the other hand, a malicious customer launches a cyber-attack on the smart meter to manipulate the reported energy generation value to the utility company in order to receive a higher payment for the transferred energy. Hence, for a malicious customer $R(d, t) = m(E(d, t))$, and the function $m(\cdot)$ is defined in a way that results in a higher

payment to the malicious customer. In practice, the function $m(\cdot)$ can be extracted based on a study of different electricity theft scenarios. The attack functions $m(\cdot)$ for various scenarios are described next.

IV.2.1 Attack Functions

The scenarios and the attack functions are described below.

1. The first attack function is given by $m_1(E(d,t)) = (1+\alpha) \times E(d,t)$. The parameter α represents the customer specific increment percentage. Each malicious customer will have a specific value for α. The customer will increase the actual hourly generated data by a percentage α which is kept constant throughout the year. Here, the value of α is randomly generated between 0 and 1 using a random number generator.

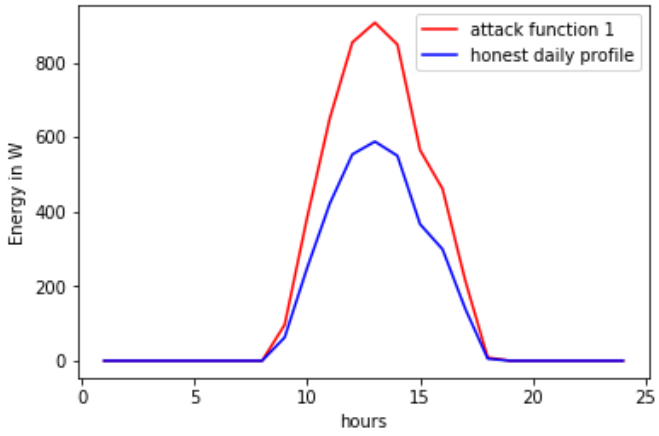

Figure 3. Malicious profile corresponding to attack function 1

2. The second attack function is given by $m_2(E(d,t)) = (1+\alpha(d,t)) \times E(d,t)$. In this scenario, α is not a constant value. It is variable with respect to date d and time t. Thus, α is a customer specific function of d and t that generates the increment percentages to increase the actual energy values.

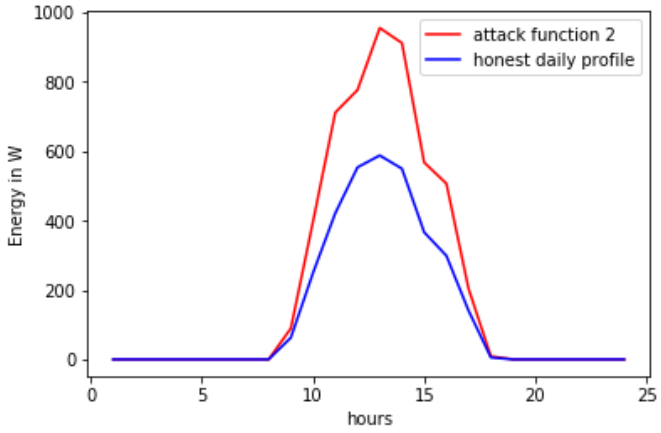

Figure 4. Malicious profile corresponding to attack function 2

3. The third attack function is given by $m_3(E(d,t)) = \alpha(d,t) + E(d,t)$. Here, α generates an integer value comparable to the actual energy values. α is basically a function of date d and time t that generates integer values which are then added to the actual energy values represented by $E(d,t)$.

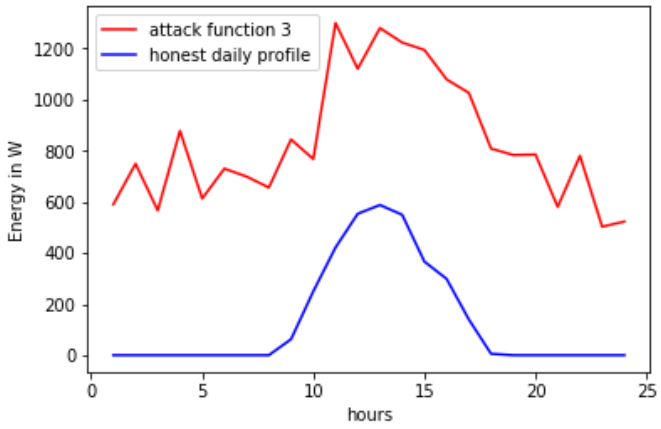

Figure 5. Malicious profile corresponding to attack function 3

4. The fourth attack function is a malicious algorithm placed in the smart meter through malware attacks. This algorithm will record the maximum hourly generated value recorded between early hours and noon and then replicate it for the hours after noon till the evening.

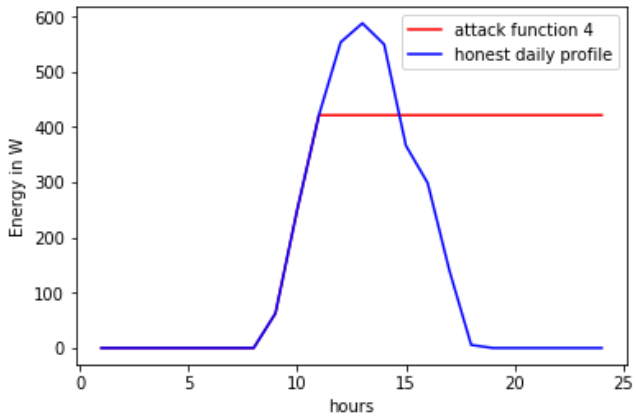

Figure 6. Malicious profile corresponding to attack function 4

Figures 3-6 depict each attack function graphically. Combined graphical representation of all attack functions is depicted in Figure 7.

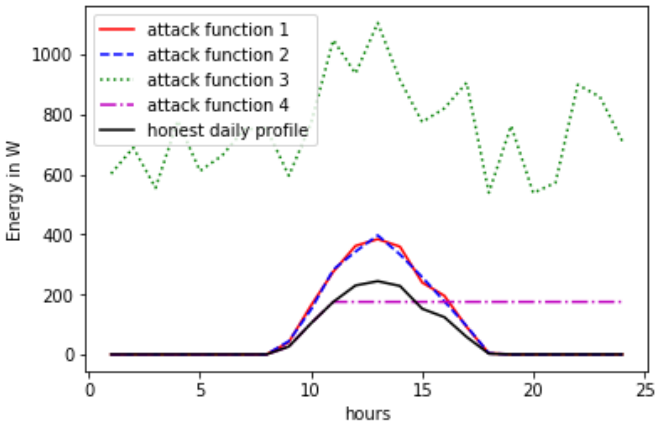

Figure 7. Malicious profiles of all attack functions

In this thesis, a generalized detector is proposed that trains on honest and malicious datasets of all customers. Hence, a combined dataset (Honest + Malicious) covering all customers will be used to model the deep-learning based detectors. But before that, the datasets (Honest + Malicious) for each of the customers must be collected. In order to generate the combined dataset for each customer, we apply the above listed cyber-attack functions on the honest energy generation matrix E_c which is the hourly generation data of a customer recorded

for 365 x 24 hours. Hence, we obtain four matrices $M_{c,i}$, each representing an attack function $m_i(\_)$. We combine E_c and each $M_{c,i}$ where i spans{1,4}, to obtain the complete data set for a customer c, namely, X_c. Each row $X_c(d, :)$ is labeled with 0 or 1 to indicate an honest or a malicious day sample, respectively. Unfortunately, X_c represents an imbalanced data set since the ratio of the honest to malicious samples is 1:4. As a result, the detector modeled using this data set will be a biased one. To overcome this drawback, the minor (honest) class is over-sampled using the adaptive synthetic sampling approach (ADASYN). This results in a balanced dataset D_c of each customer c with equal proportion of both the classes 0 and 1. The balanced datasets D_c of all customers are finally concatenated one-after-the-other to obtain the training dataset. It contains approximately 1.5×10^6 samples. This training dataset, to be referred to as D, will be used to model the Deep Neural Network based detectors.

CHAPTER V

DEEP LEARNING BASED DETECTORS

The electricity theft detectors are created using Neural Networks. The neural nets that we have considered for this project are – Feed Forward Neural Networks, GRU (Gated Recurrent Unit) and Convolutional Gated Recurrent Unit (CNN-GRU).

V.1 Motivation Behind Using Neural Networks

1. Data – The dataset *D* that will be used to train the detector is on the order of 10^6 and is quite large. A large data enables neural networks to really show their potential since they give better performance as more data is fed into them. In contrast, traditional machine learning algorithms will certainly reach a level, where more data does not really improve their performance. Figure 8 explains this perfectly.

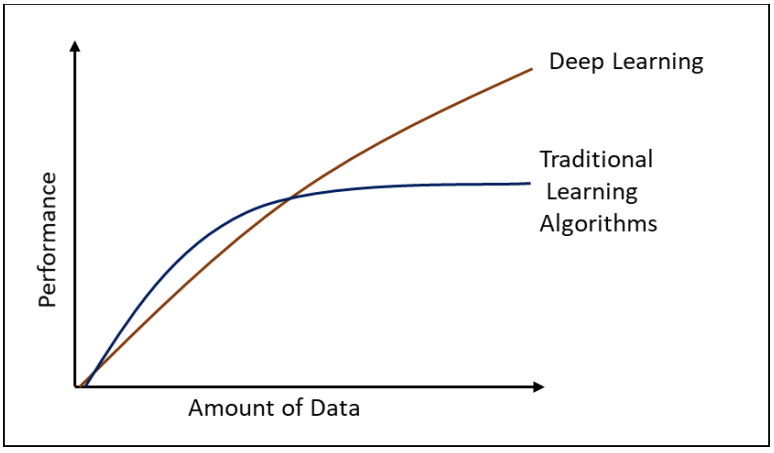

Figure 8. Plot showing performance of deep neural networks and older machine learning algorithms

2. Computational Power – Another important reason behind going for Neural Networks is the remarkable computational power available nowadays which is increasing exponentially allowing to process more data.

3. Advances in Deep Learning – A lot of research has been taking place in the area of deep learning especially around development of different algorithms like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), etc. These neural network architectures are known for their efficiency and good performance for certain specific applications. For example, RNNs are used for producing predictive results for sequential data or time-series data while CNNs yield the best performance in Computer Vision.

V.2 Brief Description of the Modeled Neural Networks

Below is a brief description about the three types of Neural Networks used to create the electricity theft detectors. The network that yields the best performance was taken up for further study and analysis.

V.2.1 Feed Forward Neural Network

Feed-forward neural networks or Deep Neural Networks (DNN), also known as multi-layered perceptron (MLP), are the basic and simplest type of neural networks. They are called feed-forward because information travels only in the forward direction, i.e., from the initial layer of neurons, through the hidden layers and finally to the output layer. A neuron is the building block of a neural network and also its basic functional unit. It is a system of inputs, weights, an activation function and outputs. Inputs to a neuron are multiplied by weights and then added to be fed to the activation function. The activation function produces the output by mapping the result to a desired range for example, between 0 and 1 or -1 and 1. This system is also referred to as a perceptron. As shown in Figure 9, it is a fundamental neural network with just two layers: the input layer and the output layer. It works according to the following simple steps. Let us assume there are m+1 inputs to the perceptron with signals x_0 through x_m and weights w_0 through w_m. Usually, the x_0 input is assigned the value +1, which makes it a bias input with $w_{k0} = b_k$.

Hence, effectively, there are m actual inputs to the neuron, i.e., from x_1 to x_m. All these inputs are added, and the result is input to the activation function.

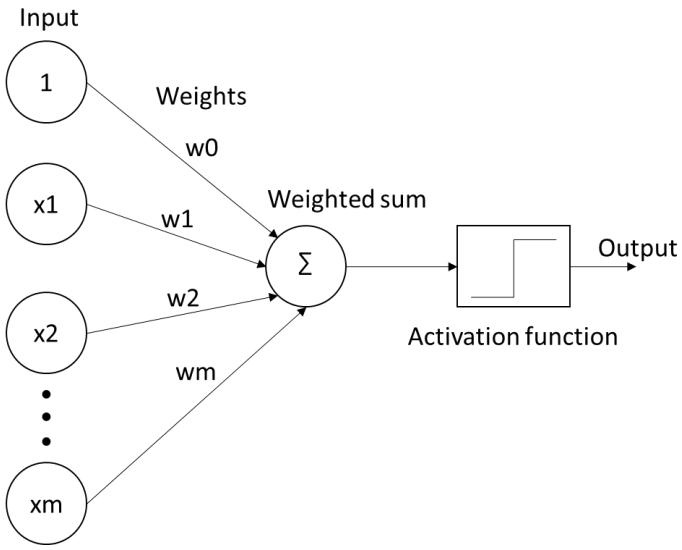

Figure 9. Perceptron

The output signal of the perceptron depends on the type of activation function used. For example, the use of the sigmoid activation function would map all inputs in the real number domain into the range of 0 to 1 or alternatively, -1 to 1.

The feed forward neural network consists of many layers: the input layer, the hidden layer and the output layer. Each layer of a feed forward neural network consists of neurons. The output of each neuron in a layer is used as input to all the neurons in the next layer. However, there is no connection between the neurons of the same layer. Thus, every neuron depends on the outputs of all the neurons in the previous layer.

V.2.2 Gated Recurrent Unit

Gated Recurrent unit (GRU) is a variant of another class of neural networks called Recurrent Neural Networks (RNNs). Recurrent Neural Networks are unique in the sense they

remember their inputs due to internal memory, which makes them perfectly suited for producing predictive results for sequential or time series data. In this research, the datasets used are time-series in nature, and therefore, RNNs are best suited for the purpose of making predictions for such data. In feed forward neural networks, there is no memory of the inputs received previously. Hence, feed forward networks exhibit poor performance in predicting the output if a sequential or time-series relationship exists in the data. However, in RNNs, information persists because of looping of the outputs. Therefore, when it makes a decision, it combines the current input and the previous output. This process allows the network to remember all the inputs it had learnt back in time and subsequently use them to make accurate predictions.

RNN's often run into a problem called vanishing gradient problem. This problem especially occurs in RNNs when the input is a large time series dataset. As more and more layers using certain activation functions are added to neural networks, the gradient of the loss function approaches zero, making the network difficult to train. For example, the sigmoid activation function maps large input values to small values between 0 and 1. Therefore, a large change in the input of the sigmoid function will result in a small change in the output. Hence, the derivative becomes small. When *n* hidden layers use an activation like the sigmoid function, *n* small derivatives are multiplied together. Thus, the gradient decreases exponentially as we move backward in the network to the front layers. A very small gradient means that the weights and biases of the initial layers cannot be updated effectively with each training session. Since these initial layers are often critical for identifying patterns in the input data, it can lead to overall inaccuracy of the whole network.

To overcome the above problem, a Gated Recurrent Unit (GRU) based detector is proposed in this thesis. GRU is an improved version of the standard Recurrent Neural Networks.

It uses two vectors called update gate and reset gate to solve the vanishing gradient problem. These two vectors basically decide which information should be passed to the output. The update gate is used to help the model decide how much of the past information needs to be passed to the future while the research gate is used to decide how much of the past information to forget.

V.2.3 Convolutional Gated Recurrent Unit

Convolutional Gated Recurrent Unit is a hybrid network of Convolutional Neural Network and Gated Recurrent Unit. It consists of a 1-dimensional CNN layer over a stack of GRU layers. Though this architecture is usually designed for sequence prediction problems with spatial inputs, like images and videos, it is being used here for time series data using a 1-D CNN layer rather than a 2-D CNN layer which otherwise would have been used for spatial inputs. Theoretically, CNN's are good at feature selection in spatial data and GRU's are good with temporal sequences. In this research, the 1-dimensional CNN acts like a trainable feature extractor for the 1-D input sequences while the GRU receives sequences of high-level features from the CNN layer to learn the temporal relationship in the data.

V.3 Modeling the Electricity Theft Detectors

This section walks through the steps involved in modeling and testing the detectors based on the three neural network types.

1. **Loading Data**: As such, this is a binary classification problem with an output label containing the two classes to which the input sequences are mapped to. The class corresponding to the malicious data/ profile is represented by 0 whereas the class corresponding to honest data/ profile is represented by 1**.** Each input to the model will be a vector *X(24,:)* containing 24 values which is the energy generated during each hour of the

day. Likewise, there will be 15×10^5 vectors forming a 'balanced dataset' with equal proportion of honest and malicious vectors.

2. **Create Network**: We create a sequential model and add layers until we get the optimal number of layers which is obtained through hyperparametric optimization. The detector architecture consists of NL hidden layers and NN neurons within each layer. The output layer consists of one neuron to predict the class (malicious or honest). The important thing here is to ensure that the input layer has enough neurons equal to the size of the input vector, i.e., 24. This was specified while creating the first layer with the *input_dim* argument and setting it to 24 for 24 input features.
3. **Hyperparametric Optimization**: Hyperparameters are properties specific to a model that are set even before the model is trained and tested on the data. Hyperparametric optimization is a technique used to find the right set of hyperparameters or the optimal hyperparameters that will yield a high testing accuracy and precision for a given model. In this research, the following hyperparameters of a neural network were optimized: number of hidden layers (NL), number of neurons in each hidden layer (NN), the Optimizer and the Activation Function. For this research, *Random Search* technique was used to perform hyperparametric optimization which is a commonly used parameter optimizing technique. This method creates random combinations of hyperparameters from a preset list of hyperparameters. These combinations are then embedded in the model to be trained and tested with data. Finally, the parameter combination that yields the best accuracy score is chosen for training the model. For training and testing the model, the PV generation profile dataset *D* was divided into two parts: Train dataset and Test dataset (see Figure 10). The train dataset was used for hyperparametric optimization and for fitting the model. The test dataset was used for

validating the fitted model. Random Search was implemented using the *Scikit-learn* function *RandomizedSearchCV*. Here random search is performed in conjunction with k- fold Cross Validation. In k-fold cross validation, the train data is divided into k equal sized subsets or k-folds. Out of the k folds, k-1 sets are used for training the model and the remaining single set is used for validating the trained model. This process is repeated until each of the k sets is validated exactly once. The result of this procedure is the mean of the k results obtained on validating the k sets. Finally, the results obtained for each parameter combination are compared to get the optimal hyperparameters.

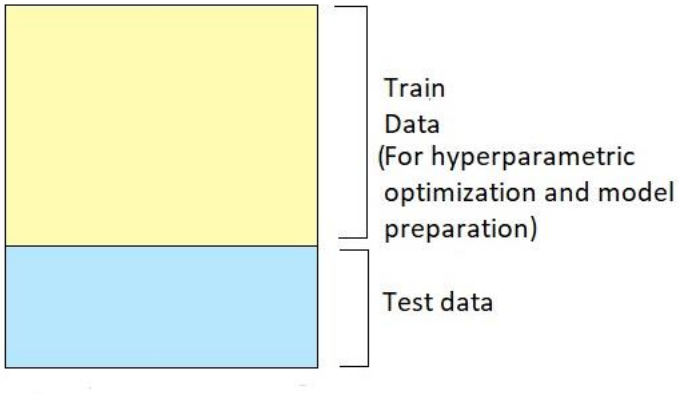

Figure 10. Partitioning of the dataset

In Random Search, the number of hyperparameter combinations to be tested for accuracy has to be explicitly provided. 'Random' refers to the random selection of parameters under each key in the parameter list. The parameter list used in this research is given as follows*: { 'nb_neurons': [64,128,256], 'nb_layers': [2,3,4], 'activation': ['relu', 'elu', 'tanh', 'sigmoid'], 'optimizer': ['rmsprop', 'adam', 'sgd', 'adagrad', 'adadelta', 'adamax', 'nadam'] }* .

4. **Model training**: The ideal hyperparameters obtained through Hyperparametric optimization are used to build the neural network followed by training it with the training dataset.

5. **Testing model**: The trained model is evaluated on the test data using the confusion matrix which is a table used to describe the performance of a classification model.

V.4 Architecture of the Detectors

V.4.1 Feed Forward Neural Network (DNN) Based Detector

A sequential model was created using the Keras Sequential API that allows layer-by-layer creation of neural networks. The initial layer or the input layer consists of 24 neurons which matches the size of the input vector. Each input vector represents daily energy generation profile of a DG unit. The elements of the input vector *X(,24)* are generated energy values per hour recorded for a period of 24 hours. The optimal number of subsequent layers and neurons in each layer is obtained through hyperparametric optimization (HPO). The Random search algorithm chooses between 4, 6 and 8 layers and 64, 126, 256 and 512 neurons (per layer). The optimal parameter set so obtained in case of Feed Forward Neural Networks is listed in Table 6.

No. of layers	8
No. of neurons	128
Activation fn.	Sigmoid
Optimizer	Nadam

Table 6. Hyperparametric set for Feed-forward neural network

The output layer consists of a single neuron to predict the output class (malicious or honest). Table 7 shows the network summary of the Feed Forward neural network generated after including the optimal parameters.

Layer (type)	Output Shape
dense_1 (Dense)	(None, 128)
dense_2 (Dense)	(None, 128)
dense_3 (Dense)	(None, 128)
dense_4 (Dense)	(None, 128)
dense_5 (Dense)	(None, 128)
dense_6 (Dense)	(None, 128)
dense_7 (Dense)	(None, 128)
dense_8 (Dense)	(None, 128)
dense_9 (Dense)	(None, 1)

Table 7. Network summary of Feed-forward neural network model

V.4.2 Gated Recurrent Unit (GRU) Based Detector

The GRU based neural network detector was created using the Keras sequential model. In GRU, the input to every layer, including the initial layer, must be 3 dimensional. Hence, the input vector *X(,24)* is reshaped into a 3D tensor *X(1,24,1)*. This 3D tensor represents one sample with only one feature and 24 observations. Likewise, there will be *N* such samples equal to the length of PV generation profile (honest + malicious) dataset.

The dimensions of the 3D tensor were decided based on the input layer of the network. For this project, a one-to-many GRU network was chosen as shown in Figure 11.

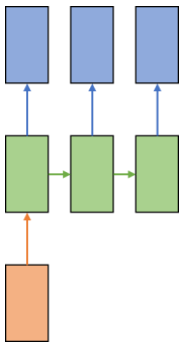

Figure 11. One-to-many gated recurrent unit model

As there is only one feature, each sample is input to the network, one observation at a time. This is done for 24 observations until the complete sample is input to the network. The optimal parameters, including the number of subsequent layers and the number of neurons per layer is obtained via hyperparameter optimization (HPO). Similar to the feed forward (FF) network, the Random search (HPO) algorithm here chooses between 4, 6 and 8 layers and 64, 126, 256 and 512 neurons (per layer). The output layer consists of a single neuron to predict the output class (malicious or honest). The optimal hyperparameter set for the GRU network is shown in Table 8.

No. of layers	4
No. of neurons	64
Activation fn.	Sigmoid
Optimizer	Adagrad

Table 8. Hyperparametric set for GRU model

The network summary of the GRU model generated after hyperparametric tuning is shown in Table 9.

Layer (type)	Output Shape
gru_1 (GRU)	(None, 1, 64)
gru_2 (GRU)	(None, 1, 64)
gru_3 (GRU)	(None, 1, 64)
gru_4 (GRU)	(None, 64)
dense_1 (Dense)	(None, 1)

Table 9. Network summary of gated recurrent unit model

V.4.3 Convolutional Neural Network – Gated Recurrent Unit (CNN-GRU) Based Detector

The CNN-GRU network was realized by a layer of 1-dimensional Convolutional Neural Network (CNN) over Gated Recurrent Unit (GRU) layers. The CNN layer was used here for feature extraction and the GRU layers for interpretation of the extracted features. This arrangement is said to improve the performance of the detector significantly. The input to this network is also a 3D tensor X(1,24,1). Like GRU, the input CNN layer accepts the sample, one observation at a time. Hyperparameter optimization (HPO) was performed to generate the optimal hyperparameters. They are listed in Table 10.

	CNN	GRU
No. of layers	1	4
No. of neurons	64	64
Activation fn.	Relu	Sigmoid
Optimizer		Rmsprop

Table 10. Hyperparametric set for CNN-GRU model

These parameters were embedded in the arrangement to provide the network topology shown in Table 11.

Layer (type)	Output Shape
conv1d_1 (Conv1D)	(None, 57, 64)
max_pooling1d_1 (MaxPooling1	(None, 14, 64)
gru_1 (GRU)	(None, 14, 64)
gru_2 (GRU)	(None, 14, 64)
gru_3 (GRU)	(None, 14, 64)
gru_4 (GRU)	(None, 64)
dense_1 (Dense)	(None, 1)

Table 11. Network summary of CNN-GRU model

V.5 Performance of The Detectors

The three-deep learning-based detectors were evaluated based on two performance metrics: *Detection Rate* and *False Alarm Rate*, respectively. The detection rate (DR) measures the fraction of correctly detected malicious samples, while the false alarm (FA) measures the fraction of honest samples that are falsely identified as malicious. Both these metrics are derived from the confusion matrix. As shown in Table 12, Confusion matrix is a specific table layout that describes the performance of a classification model on a test data for which the class value is already known. In this research, the *Scikit-learn* library has been used to generate the confusion matrix.

	Predicted: Negative	Predicted: Positive
Actual: Negative	True Negatives (TN)	False Positives (FP)
Actual:Positive	False Negatives (FN)	True Positives (TP)

Table 12. Confusion matrix

The negative class is represented by 0 and the positive class is represented by 1**.** From the confusion matrix, the DR and FA rates can be calculated using the following formulas: *Detection Rate = TP/ (TP + FN)* and *False Alarm Rate = FP/ (TN + FP).*

An efficient detector should ideally have a high DR and a low FA rate. The DR and FA rates of the 3 detectors are listed in Table 13.

S. No.	Network	Data	Parameters				Test Results (on test data)	
			NN	NL	Optimizer	Activation	DR	FA
1	DNN	Meter Data	128	8	Nadam	Sigmoid	90	2
2	GRU	Meter Data	64	4	Adagrad	Sigmoid	91	2.6
3	CNN + GRU	Meter Data	CNN:64, GRU:64	CNN: 1, GRU:4	Rmsprop	CNN: relu, GRU:sigmoid	94.6	1.7

Table 13. Detection and false alarm rates of the detectors

V.5.1 Remarks

It is perceived from the above table that out of the three detectors, the CNN-GRU based detector is the most effective as its detection rate is the highest (94.6%) and its false alarm rate (1.7%) is sufficiently low. Therefore, it is inferred that the hybrid network of Convolutional Neural Network and Gated Recurrent Unit provides greater efficiency and accuracy in prediction. The enhanced performance is attributed to the combined roles of CNN and GRU in this network. The raw data is represented by different features which are selected by CNN and the same data also has temporal properties for which GRU is used.

CHAPTER VI

TEST OF HYPOTHESIS

VI.1 Hypothesis

The neural network-based detectors modeled above were trained on honest and malicious distributed PV generation smart meter data, also referred to as PV generation profile of the households. This data is received from smart meters, which is the only source of this data. The detectors learned the different patterns observed in this data, correlated normal and abnormal patterns and created efficient two-class classifiers. Their performance was observed to be satisfactory and also met the expectation of this research. Thereafter, it was inferred that the CNN-GRU model is the most effective one as it provided the best detection and false alarm rates. But, even with such good detection and false alarm rates, the possibility of a false alarm or a malicious profile going undetected still exists as the ideal detection (100%) and false alarm (0%) rates could not be achieved. However, these rates can be further improved by involving other relevant data. In this research, it is hypothesized that utilities can also make use of data other than the received PV Generation data to detect electricity thefts. For instance, the solar irradiation data recorded at the utilities can be correlated with the generated power data coming from DG units for a more accurate detection of electricity thefts. It is naturally expected that PV generation profile of DG units follows the solar irradiation profile. Hence, there should exist a relationship between these two temporal sequences which can be captured. In this research, this relationship has been utilized to detect thefts using Keras functional API which is discussed in detail in the following section.

Most models take a single data type as input. However, it is expected that a model that combines multiple data streams can provide a better predictive performance. In this view, a detector that combines multiple data for achieving improved detection is envisaged. The CNN-GRU detector which provided the best detection performance will further add Irradiation Data for an improved theft detection. The idea behind this proposed model is illustrated in Figure 12.

Honest PV Data	Solar Irradiance (honest from utility)	Target Label (Honest)
		0
		0
		0
		0
Malicious PV Data	Solar Irradiance (honest from utility)	Target Label (Malicious)
		1
		1
		1
		1

Figure 12. Improved theft detection using multiple datasets

Description: The proposed network will be trained on honest and malicious PV generation profiles of the households while utilizing corresponding irradiation data as metadata. This metadata supplements the detector with additional information about the primary data. The irradiation data is honest because it is recorded by the AWS (Automatic Weather Station) at the utility and is not received from the smart meters. The correlation between honest generation data and honest irradiation data as well as between malicious generation data and honest irradiation data will be learned by the proposed network. This will yield a better performance.

VI.2 Keras Functional API

The proposed arrangement was realized using the Keras Functional API. Keras functional API is another way of creating classification models that offers a lot more flexibility than the commonly used Keras sequential API. Keras sequential API is restricted in a way that it only allows you to create networks layer-by-layer. On the other hand, Keras functional API allows to build complex models with shared layers as well as multi-input and multi-output models. Models are defined by creating instances of layers and connecting them directly to each other in pairs followed by defining the specific layers that will act as the inputs and outputs to the model. This has made it really possible to reuse the already trained models which is a very useful feature of this API. A sample multi-input multi-output neural network created using the functional API is shown in Figure 13.

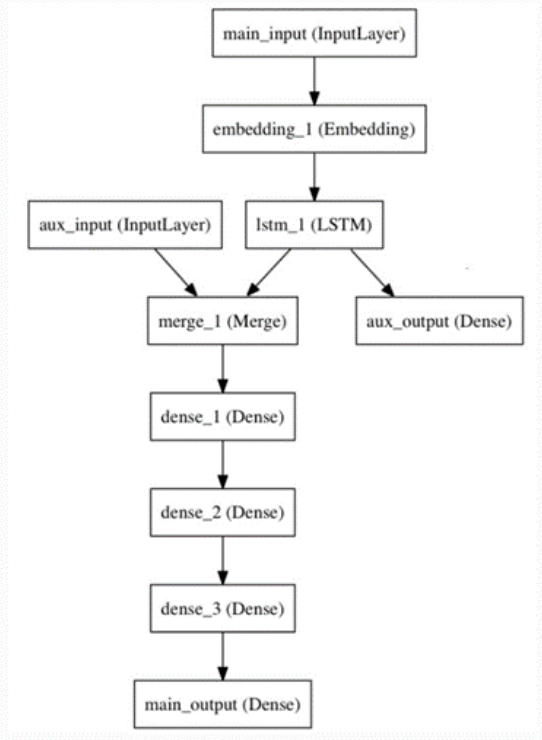

Figure 13. Network topology of a multi-input multi-output model

VI.3 Modeling an Improved Detector Based on Multiple Datasets

After having identified the prospect of including additional information that is, irradiation data, a new detection architecture based on the CNN-GRU detector was designed using the Keras functional API. The proposed detector was designed using the CNN-GRU detector because it gave the best detection and false alarm rates. This model adds Irradiation data (as auxiliary input) as depicted in the Figure 14.

The main input to the model will be the PV generation data itself. This data is modeled by the subsequent layers which are similar to the original CNN-GRU based detector. Like the CNN-GRU detector, the input layer is a CNN layer followed by GRU layers. At the end of the sixth GRU layer, the network receives an auxiliary input which is the Irradiance data. Here the irradiance data is merged with the output of the CNN-GRU hybrid layers and the resultant is modeled by a stack of dense layers. Dense layers are regular layers of neurons in a network. The last layer of this network is the main output layer which is another dense layer containing only one neuron which is the output neuron. This output neuron predicts the output class (malicious or honest).

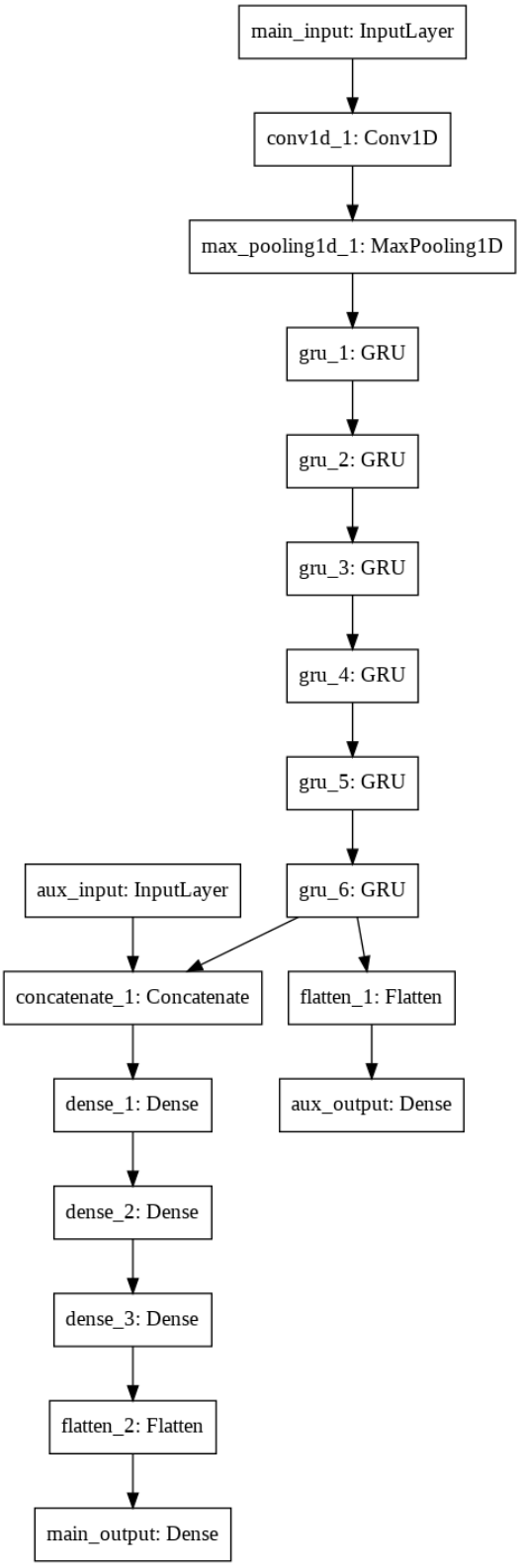

Figure 14. Network topology of the proposed CNN-GRU based detector adding Irradiance data

Like the CNN-GRU detector, this network also accepts a 3D tensor as input which is referred to as a sample. The optimal number of GRU layers and the number of neurons in each layer is obtained by Hyperparameter optimization (HPO) using Random Search. Table 14 shows the hyperparameter set of this architecture.

	CNN	GRU
No. of layers	1	6
No. of neurons	64	64
Activation fn.	Relu	Sigmoid
Optimizer		Rmsprop

Table 14. Hyperparametric set of the proposed CNN-GRU based detector adding Irradiance data

V.3.1 Performance of The Proposed Detector

The revised CNN-GRU detector that adds Irradiance data was tested and validated using the confusion matrix. Detection Rate and False Alarm rates were used to determine its performance. The results are described in the Table 15.

		Parameters				Test Results			
Network	Data	NN	NL	Optimizer	Activation	DR(Main)	FA(main)	DR(Aux)	FA(Aux)
CNN + GRU (using function API)	Meter Data + Irradiance	CNN:64, GRU:64	CNN: 1, GRU:6	rmsprop	CNN: relu GRU:Sigmoid	99.1	0.9	94.08	1.3

Table 15. Results of the revised CNN-GRU model

VI.3.2 Remarks

It is observed that the Detection rate (main) and False alarm rate (main) of the proposed detector is highest (99.1 %) and lowest (0.9 %), respectively. Please note in Figure 14 that the proposed architecture first trains on the honest and malicious data before adding the irradiance data. The output of this part of the complete architecture is shown as aux_out in Figure 14. This

part of the complete architecture is nothing but the CNN-GRU detector discussed previously that trained on a single dataset. The detection and false alarm rates for this part represented by DR(Aux.) and FA(Aux.) in Table 15 are 94.08% and 1.3%, respectively. These values are approximately the same as the detection and false alarm rates of the CNN-GRU detector modeled previously.

CHAPTER VII

CONCLUSION

VII.1 Summary

In the hypothesis, we envisaged that the performance of a classifier trained to predict two or more classes in a dataset can be significantly improved if we supplement the training data (containing the two classes) with metadata. The metadata should not only be relevant but should also give additional information about the training data. In this thesis, we identified solar irradiance data as the metadata and that it should have some correlation with the generation profiles (honest) of the DG units. This was inferred from the fact that the daily generation profile of the households in an area must follow the solar irradiation profile of that area. This assumption was also confirmed through observation of the honest generation dataset and irradiance data. This correlation was used to identify the irregularities in the combined Honest and Malicious PV dataset which ultimately helped achieve a classifier that classifies honest and malicious generation profiles with greater accuracy.

The research began with cleaning and processing the honest energy generation dataset. Then, the dataset was subjected to certain attack functions for manipulating honest data thus, creating a malicious dataset. This malicious data was assumed to be similar to the actual malicious data generated by malicious customers. Then, the honest and the malicious data were mixed together, normalized and subsequently used to train three neural networks, namely Feed forward (FF), Gated Recurrent Unit (GRU) and a hybrid network of CNN and GRU called Convolutional Gated Recurrent Unit (CNN-GRU). A detailed analysis of these neural networks and their performance on the detection was presented. Thereafter, a unique detector that

correlates multiple datasets was created using Keras Functional API. For this thesis, the two datasets used to train the proposed detector are the PV generation data (honest + malicious) and Irradiance data (metadata). The process map in Figure 15 shows the steps undertaken to obtain the ideal detector offering the best electricity-theft detection performance.

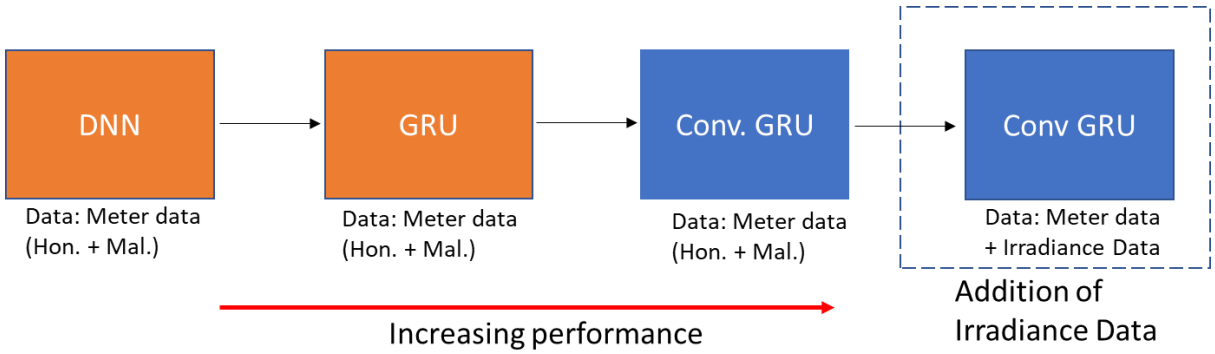

Figure 15. Ideal detector for electricity-theft detection

The convolutional-GRU detector that trained on PV Generation data and subsequently added Irradiance data delivered the best performance with a high detection rate and low false alarm rate.

VII.2 Possible Future Research Directions

The concept of combining multiple datasets for improving electricity-theft detection can be further extended to include other relevant datasets. In this research, we supplemented the PV generation profiles with corresponding irradiance profiles to make use of the relationship between them which was inferred based on facts (the energy generated by panels must follow irradiance) as well as analysis of the available datasets. Let us assume a scenario where the households/ DG units immediately consume the generated PV energy and transfer the excess to the grid. This is based on the presumption that there is no provision for storage of energy in the individual DG units. Since the energy generated by the households is immediately consumed,

there must be a correlation between the excess PV energy that they collectively transfer to the utilities and the generation data reported by the DG units. This correlation can be captured to obtain an improved detection performance. The utilities receive the SCADA readings from the buses. These bus SCADA readings measure the net energy generated by the households (DG units) connected to the buses. Hence, there must be a relationship between the bus SCADA readings, reflecting the excess generated power received by the utilities and the reported smart meter readings. This relationship can be further explored. The detector trained on honest and malicious smart meter data can also combine the bus SCADA readings in order to obtain a further enhanced performance on detection. It should capture the correlation between the three quantities namely- Honest and Malicious PV generation Data (Primary data), Irradiance Data and the bus Scada readings.

REFERENCES

[1] Analysis: Electricity theft in South Africa. (2017, June 27). Retrieved from https://www.smart-energy.com/features-analysis/electricity-theft-south-africa/

[2] Theft of Electricity. Retrieved from https://en.wikipedia.org/wiki/Theft_of_electricity

[3] L. G. Arango, E. Deccache, B. D. Bonatto, H. Arango, P. F. Ribeiro and P. M. Silveira, "Impact of electricity theft on power quality," 2016 17th International Conference on Harmonics and Quality of Power (ICHQP), Belo Horizonte, 2016, pp. 557-562.

[4] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni and N. Gudi, "Measures and setbacks for controlling electricity theft," North American Power Symposium 2010, Arlington, TX, 2010, pp. 1-8.

[5] Advanced metering Infrastructure (AMI). (2010, March). Retrieved from https://internetofthingsagenda.techtarget.com/definition/advanced-metering-infrastructure-AMI

[6] Advanced Metering Infrastructure and Customer Systems: Results from the Smart Grid Investments Grant Program. (2016, September). Retrieved from https://www.energy.gov/sites/prod/files/2016/12/f34/AMI%20Summary%20Report_09-26-16.pdf

[7] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," 2011 10th International Conference on Environment and Electrical Engineering, Rome, 2011, pp. 1-4.

[8] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong and S. Sastry, "A game theory model for electricity theft detection and privacy-aware control in AMI systems," 2012 50th Annual

Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, 2012, pp. 1830-1837

[9] C. Lin, S. Chen, C. Kuo, and J. Chen, "Non-cooperative game model applied to an advanced metering infrastructure for non-technical loss screening in micro-distribution systems," IEEE Trans Smart Grid, vol. 5, no. 5, pp. 2468-2469, Sept. 2014.

[10] T. Zhan et al, "Non-technical loss and power blackout detection under advanced metering infrastructure using a cooperative game-based inference mechanism," IET Generation, Transmission, & Distribution, vol. 10, no. 4, pp. 873-882, Oct. 2015.

[11] S. K. Singh, R. Bose and A. Joshi, "Entropy-based electricity theft detection in AMI network," IET Cyber-Physical Systems: Theory & Applications, vol. 3, no. 2, pp. 99-105, 6 2018.doi: 10.1049/iet-cps.2017.0063

[12] C. Ramos, Nunes de Sousa, P. Andrá, F. João, and A. Falcão, "A New Approach for Nontechnical Losses Detection Based on Optimum-Path Forest," IEEE Transactions on Power Systems, vol. 26, pp. 181 – 189, 2011. 10.1109/TPWRS.2010.2051823.

[13] E. Ângelos, O. Saavedra, C. O. Cortes, and A. Souza, "Detection and Identification of Abnormalities in Customer Consumptions in Power Distribution Systems", IEEE Transactions on Power Delivery, vol. 26, pp. 2436-2442, 2011. 10.1109/TPWRD.2011.2161621.

[14] J. Nagi, K. S. Yap, S. K. Tiong, S. K. Ahmed and M. Mohamad, "Nontechnical Loss Detection for Metered Customers in Power Utility Using Support Vector Machines," IEEE Transactions on Power Delivery, vol. 25, no. 2, pp. 1162-1171, April 2010.

[15] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar and S. Mishra, "Decision Tree and SVM-Based Data Analytics for Theft Detection in Smart Grid," IEEE Transactions on Industrial Informatics, vol. 12, no. 3, pp. 1005-1016, June 2016.

[16] Y. He, G. J. Mendis and J. Wei, "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2505-2516, Sept. 2017.

[17] V. Ford, A. Siraj and W. Eberle, "Smart grid energy fraud detection using artificial neural networks," 2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG), Orlando, FL, 2014, pp. 1-6.

[18] M. Ismail, M. Shahin, M. F. Shaaban, E. Serpedin and K. Qaraqe, "Efficient detection of electricity theft cyber attacks in AMI networks," 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, 2018, pp. 1-6.

[19] M. Nabil, M. Ismail, M. Mahmoud, M. Shahin, K. Qaraqe, and E. Serpedin, ``Deep Recurrent Electricity Theft Detection in AMI Networks with Random Tuning of Hyper-parameters", 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, China, Aug. 2018, arXiv:1809.01774v1 [cs.AI].

[20] H. He, Y. Bai, E. Garcia, and S. Li, "ADASYN: Adaptive synthetic sampling approach for imbalanced learning," in Proc. of IEEE International Joint Conference on Computational Intelligence, 2008, pp. 1322–1328.

[21] IEEE 123 Node Test Feeder. (Updated 2010, September 15). Retrieved from http://sites.ieee.org/pes-testfeeders/resources/