CMPT318 Fall 2020
Term Project

Roshan Kakadiya

Gursmeep Singh Syan

Sehajvir Singh Pannu

Abstract

A statistical analysis of individual household electricity consumption was performed for the purpose of finding vulnerability of todays grid systems versus the threat of cyber-attacks.

As asked of us in the Project Roadmaps , we strive to evaluate the usage of Hidden Markov Models to detect a cyber incursion and while we also consider the usage of Reinforcement Learning as an online intrusion detection mechanism to encounter the problem of increasing threats of cyber-attacks .

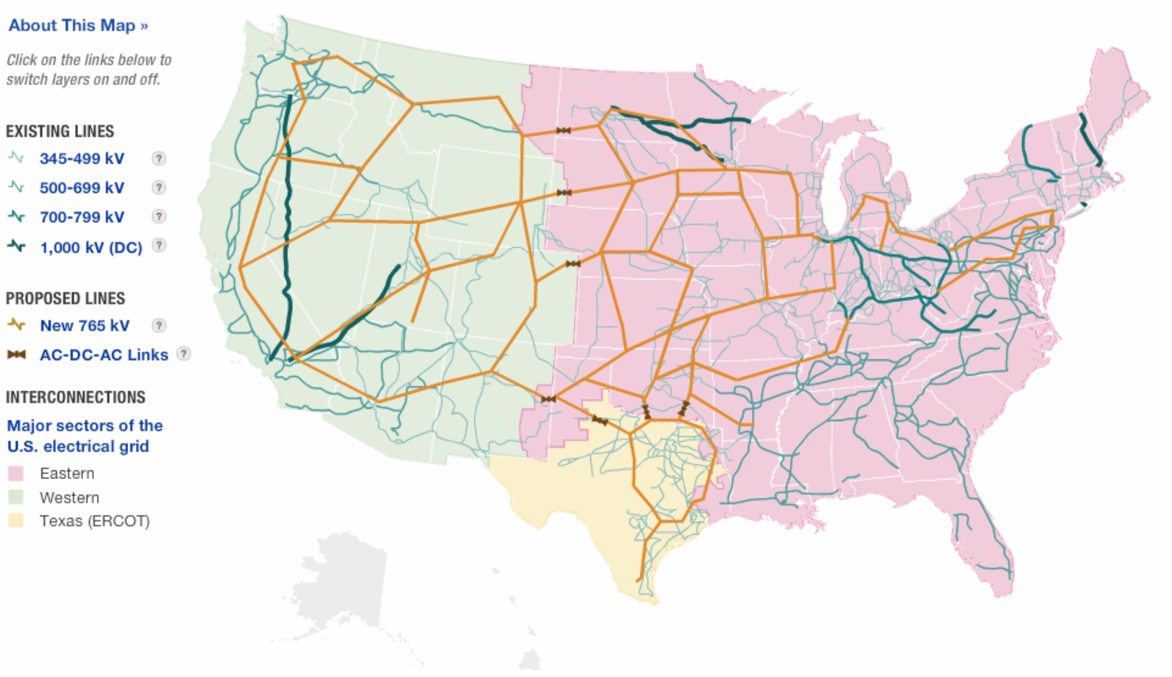
Table of Contents

List of Figures

1.1 Introduction

For their continuous service, energy grids, intelligent transportation networks, public water utilities, oil and gas pipelines and other vital infrastructure routinely depend on automated power.

The aim of this project is to evaluate electrical grid data using a dataset obtained from the observation of household energy use with the primary objective of reducing the risk of human threats by encouraging early warning and minimizing a wide range of disasters. Situational awareness is a key concept that involves continuous identification of various types of anomalies capable of distinguishing an attack from noise such as power outages, natural disasters and many more, with suitable probabilistic models.



The project examines behavior-based intrusion detection techniques used for cyber situational awareness of automated control processes in light of increasing cyber threats, especially advanced persistent threats, and existing vulnerabilities that expose critical infrastructure to a variety of adversarial scenarios such as the ever impending threat of APTs in SCADA system.

The required power supply to an electric circuit depends on the active power (P) - real electrical resistance power consumption in circuits
reactive power (Q) - imaginary inductive and capacitive power consumption in circuits
The required power supply is called the apparent power (S) and is a complex value that can be expressed in a Pythagorean triangle relationship, the apparent power is the power supplied to the electric circuit—typical from a power supplier to the grid—to cover the real and reactive power consumption in the loads.

But a major observation shall be that he use of AC power makes the need of hundreds of generators connected to the grid to be maintained in synchronization. This means producing AC power at exactly the same frequency and the same phase so that the power from many sources can be summed to meet the demand is absolutely necessary.

1.2 Knowledge Background

Throughout this course, we have been assessing and analysing data with the help of techniques that require some complexity but are very intuitive.

We have been using raw data to analyse how various trends occur in a given dataset.Then using the same dataset we have been plotting graphs for things like correlation values between different variables.

The bulk of this project has been on training and testing Hidden Markov Models using Univariate and Mutivariate Analysis Methods while also detecting anomalies in the given datasets. A heavy reliance on R programming language and RStudio for the packages to undertake the above mentioned tasks has been the case for this project.

2.1 Datasets

Variables	Description
Date	Date in dd/mm/yyyy format
Time	Time in hh:mm:ss format
Global_active_power	Household global minute-averaged active power (kW)
Gobal_reactive_power	Household global minute-averaged reactive power (kW)
Voltage	Minute-averaged voltage (V)
Global_intensity	Household global minute-averaged current intensity (A)
Sub_metering_1	appliance energy usage (Wh)
Sub_metering_2	appliance energy usage (Wh)
Sub_metering_3	appliance energy usage (Wh)

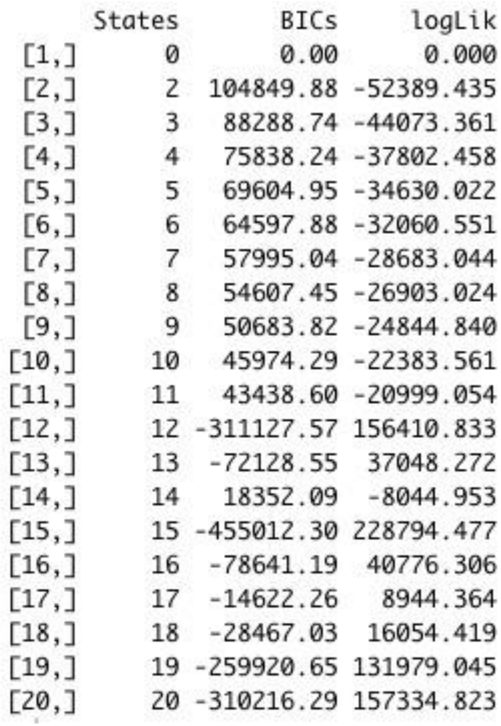
2.2 Correlation

	(a)	(b)	(c)	(d)	(e)	(f)	(g)
(a)Global_active_power	1.000	0.099	0.310	0.683	0.167	0.321	0.313
(b)Global_reactive_power	0.099	1.000	-0.183	0.318	0.230	0.095	0.064
(c)Voltage	-0.310	-0.183	1.000	-0.442	-0.231	-0.216	-0.169
(d)Global_intensity	0.683	0.318	-0.442	1.000	0.478	0.464	0.503
(e)Sub_metering_1	0.167	0.230	-0.231	0.478	1.000	0.065	0.071
(f)Sub_metering_2	0.321	0.095	-0.216	0.464	0.065	1.000	0.052
(g)Sub_metering_3	0.313	0.064	-0.169	0.503	0.071	0.052	1.000

CORRELATIONS MATRIX

The response variable we chose was Global Active Power as this was a measure of the true power consumption in the households. This response variable was used to calculate a suitable time window which we chose to be Wednesday Mornings. Furthermore , we used this newly created data to train and test the HMMs for Univariate analysis with three different datasets which included anomalies . Similarly , while conducting the Multivariate analysis for HMMs , we used the values of Global Active Power along with Sub Metering 1 and Sub Metering 3 as the variables to model our data and then test it against anomalies.

2.3 Univariate HMM



```
      States       BICs     logLik
 [1,]      0       0.00      0.000
 [2,]      2  104849.88 -52389.435
 [3,]      3   88288.74 -44073.361
 [4,]      4   75838.24 -37802.458
 [5,]      5   69604.95 -34630.022
 [6,]      6   64597.88 -32060.551
 [7,]      7   57995.04 -28683.044
 [8,]      8   54607.45 -26903.024
 [9,]      9   50683.82 -24844.840
[10,]     10   45974.29 -22383.561
[11,]     11   43438.60 -20999.054
[12,]     12 -311127.57 156410.833
[13,]     13  -72128.55  37048.272
[14,]     14   18352.09  -8044.953
[15,]     15 -455012.30 228794.477
[16,]     16  -78641.19  40776.306
[17,]     17  -14622.26   8944.364
[18,]     18  -28467.03  16054.419
[19,]     19 -259920.65 131979.045
[20,]     20 -310216.29 157334.823
```

Figure 1

State 14 is the best for our Univariate Hidden Markov Model Analysis and Anomaly detection

The difference in log likelihood values for train vs test data was 728.91

Similarly the differences in log likelihood values for train vs anamolies 1 , 2 ,3 was 6789.68 , 18762.04 and 21909.71 respectively

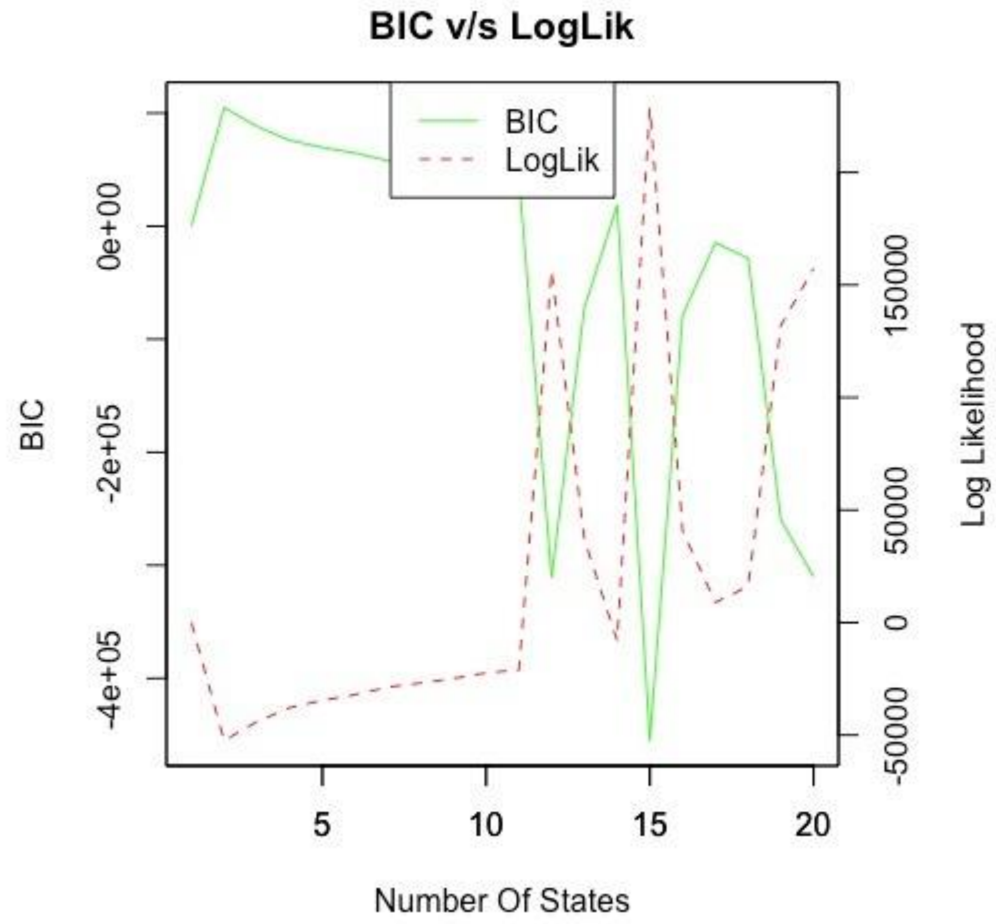
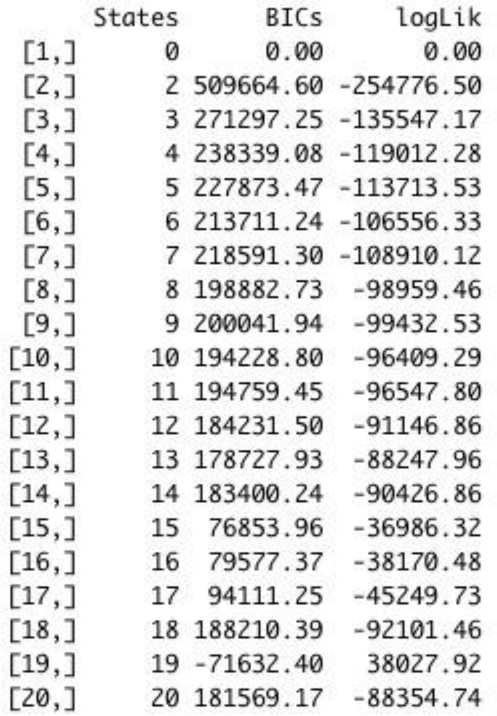

BIC v/s LogLik
BIC
LogLik
BIC
0e+00
-2e+05
-4e+05
Log Likelihood
-50000
0
50000
150000
5
10
15
20
Number Of States

Figure 2

2.4 Multivariate HMM



```
      States       BICs     logLik
 [1,]      0       0.00       0.00
 [2,]      2 509664.60 -254776.50
 [3,]      3 271297.25 -135547.17
 [4,]      4 238339.08 -119012.28
 [5,]      5 227873.47 -113713.53
 [6,]      6 213711.24 -106556.33
 [7,]      7 218591.30 -108910.12
 [8,]      8 198882.73  -98959.46
 [9,]      9 200041.94  -99432.53
[10,]     10 194228.80  -96409.29
[11,]     11 194759.45  -96547.80
[12,]     12 184231.50  -91146.86
[13,]     13 178727.93  -88247.96
[14,]     14 183400.24  -90426.86
[15,]     15  76853.96  -36986.32
[16,]     16  79577.37  -38170.48
[17,]     17  94111.25  -45249.73
[18,]     18 188210.39  -92101.46
[19,]     19 -71632.40   38027.92
[20,]     20 181569.17  -88354.74
```

Figure 3

State 15 is the best for our Multivariate Hidden Markov Model Analysis and Anomaly detection

The difference in log likelihood values for train vs test data was 5789.68

Similarly the differences in log likelihood values for train vs anamolies 1 , 2 ,3 was 9613.49 , 10562.59 and 16383.90 respectively

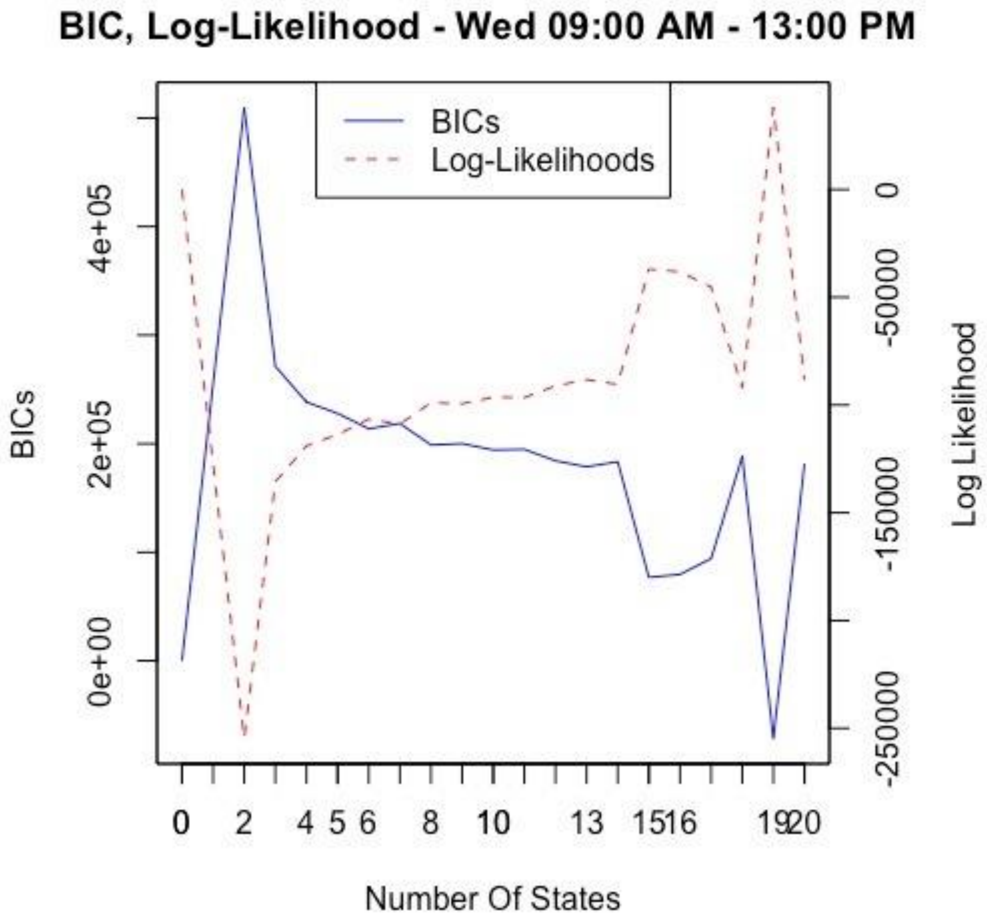

BIC, Log-Likelihood - Wed 09:00 AM - 13:00 PM
BICs
Log-Likelihoods
BICs
0e+00
2e+05
4e+05
Log Likelihood
0
-50000
-150000
-250000
0
2
4
5
6
8
10
13
15
16
19
20
Number Of States

Figure 4

2.5 Principal Component Analysis

Unfortunately, our code did not work for calculating the PCAs where we were trying to aggregate the mean of each of the response variables for a particular day in the dataset for a year. This mean was to be calculated during one time interval which was to be specified by us.

But due to there being scaling errors in our code where some dates gave a constant/zero scaling factor in pcrcomp function of the PCA calculation, we were unable to have any form of findings for this part of the project.

3.1 Technical Essay

Reinforcement learning and its Application as an online machine learning method for Intrusion Detection.

Reinforcement learning is an area of Artificial Intelligence. It has emerged as an efficient instrument to develop artificially intelligent systems and solve problems with sequential decision making. In recent years, reinforcement learning has made many remarkable breakthroughs and has been able to reach beyond human level in many fields for example it is able to play and win different games. The increasing vulnerability to cyber attacks identified as any sort of offensive maneuver carried out by one or more computers to target computer information systems, network infrastructures or personal computer devices which is followed by recent advanced innovations such as 5G cellular network, cloud computing, software defined network , fog computing, etc. Economic rival or state sponsored attackers cold instigate cyber attacks. The advancement of cyber security technology has therefore been crucial in minimizing and preventing the consequences of these attacks. In the last two decades, companies have evolved different tools and strategies to secure networks and systems against various security threats, such as access control protocols, user authentication, and firewalls. While these solutions prevent outsiders from unauthorized entry, they are not immune to insider attacks. The intrusion detection system (IDS) was therefore designed to serve as the second line of defense to protect intruders from information loss. It is used to track traffic from hostile networks and device use that is invisible to the standard firewall. This includes exposed-service network attacks, device attacks, host-based attacks such as unauthorized logins and access to sensitive data. Historically, reinforcement learning was successful in solving same control system issues but it has increasing variety of applications nowadays. And one of them is cybersecurity intrusion system.

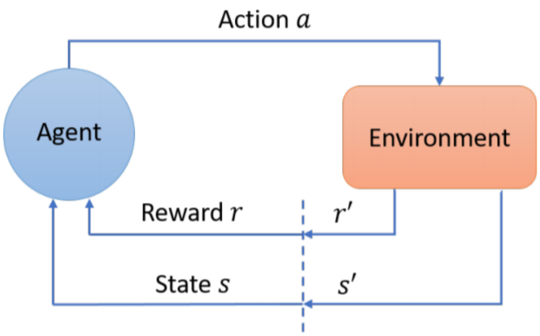
AI, especially machine learning has been used in cyberspace for attacking as well as defending. Machine learning is used on attacker side to compromise defensive tactics. On the cyber security side, in order to adaptively avoid and mitigate the impacts or losses that have occurred, machine learning used to put up good resistance against security threats. Among these machine learning applications many supervised as well as unsupervised methods are used for intrusion detection. Without using their labels, unsupervised techniques learn from example based on data labels. A statistical analysis indicated that 62% of attacks have 3been detected since causing substantial form of cyber attacks. Researchers also classified IDS as signature-based systems and anomaly-based systems. In this essay we will discuss about anomaly based systems. Based on a deviation from a collection of base-line functionalities, the anomaly-based device detects malicious behavior. They are capable of detecting zero-day attacks on these systems. The main drawback of anomaly-based systems, however is their uncertainty about accurate detection of legitimate traffic.

The closest form of human learning is reinforcement learning since it can learn from its own experience by discovering and manipulating the unknown world. Reinforcement learning can model an autonomous agent to take sequential actions optimally. Reinforcement learning shows excellent suitability for cyber security applications where cyber attacks are increasingly complex, swift and omnipresent. Its is a machine learning methodology that incorporates two disciplines to solve problems effectively that can not be independently solved either discipline. It is an orthogonal technique that tackels a particular more complicated problem. To produce efficient machine learning systems, reinforcement learning combines the field of dynamic programming and supervised learning. The machine is simply given a goal to accomplish in reinforcement learning by trial and error method where it encounters with its environment, the machine then learns how to achieve that goal.

Consider the dilemma of learning to ride a bicycle to provide the logic behind reinforcement learning. The objective given to the RL system is simply to ride the bike without falling over. The RL device starts riding the bicycle in the first trial and performs a series of acts that result in the bicycle being inclined 45 degrees to the right. Two acts are possible at this point: turning the handle bars left or turning them right. The RL device flips the bars of the handle to the left and crashes to the ground immediately, earning a negative reinforcement. When tilted 45 degrees to the right, the RL scheme has just learned not to turn the handle bars left. The RL mechanism performs a sequence of acts in the next trial that lead to the bicycle tilting 45 degrees to the right again. The RL device knows that the handle bars are not turned to the left, so the only other logical action is carried out which is to turn right. It falls instantly to the ground, receiving a powerful negative reinforcement again. At this point, the RL system has not only discovered that when tilted 45 degrees to the right, turning the handle bars right or left is bad, but that the' condition' of being titled 45 degrees to the right is bad. The RL device would finally learn how to avoid the bicycle from ever falling over by doing enough of these trial-and-error encounters with the environment.

By communicating directly with the environment, RL characterizes an agent by generating its own learning experiences. RL is defined by state, action, and reward principles. It is an approach to trial and error in which the agent acts at each point, creating two changes: the current state of the environment is changed to a new state, and the agent receives a reward or punishment from the environment. The reward is a feature, given a state, that can tell the agent how good or bad an action is. The agent learns to take more positive actions and eventually weed out bad actions, based on earned rewards.

Markov decision process is a way to formalize the process of sequential decision making. We can thus formalize the issue of reinforcement learning with the finite Markov decision method. The agent, the environment, the states, the actions and the rewards are 5 components of the Markov decision process. In the environment, agents take action on the basis of the existing state of the environment. The environment shifts to another state after every action. The agent receives a reward for the prior state's behavior. In an episode or a certain number of steps, the agent's objective is to maximize the cumulative reward it receives.



The above figure describes the interactions, defined by state, behavior and reward, between the agent and its environment in reinforcement learning. The agent will take optimal action on the basis of the current state s and reward r, resulting in changes in states and rewards. To decide the next step, the agent then receives the next state s' and the reward r' from the environment, making an iterative agent-environment interaction process.

Q-learning is a reinforcement learning algorithm in which, during the transition from one state to another the agent learns the policy. Here by examining all possible, feasible behavior linked to different states of the agent, the optimal set of policies is synthesized. Based on the next state and next greedy action, this algorithm uses Q-value which is modified. The Q-function basically takes different arguments as a vector of state (s), vector of action (a), reward (r), and rate of learning (γ). Subsequently, it defines the discount factor for the Q-value measure. However, due to the high dimensionality constraint, the Q-learning-based model computes poorly in the presence of a large state space.

One of the application of machine learning method for intrusion detection is Support vector machine (SVM). It is a supervised machine learning model that uses classification algorithms for two group classification problems, regression and even outlier detection. In the mid-1990s, support vector machinery (SVM) was introduced. Basically, the idea behind SVM for intrusion detection is to use the training data as a definition of only the usual class of objects or recognized as non-attack in the detection framework of intrusion, and thus assume the remainder as anomalies. The classifier constructed by the methodology of support vector machines discriminates against the input space in a finite region where the normal objects are contained, and the exceptions are presumed to contain all the rest of the space. By drawing a straight line between two classes, the linear SVM classifier operates. Both data points falling on one side of the line are labeled as one class and all the points falling on the other side are labeled as the second class. But it has deal in choosing the best line among infinite lines. So to overcome this LSVM algorithm is used where it selects a line that not only separates the two classes but stays as far away from the closest samples as possible.

Because of its generality, reinforcement learning appeals to many researchers. This technique will theoretically help any problem domain that can be cast as a Markov decision process. In fact, reinforcement learning is not seen by many researchers as a process, but rather as a specific type of problem. Reinforcement learning is an extension of classical dynamic programming in that the set of issues that can practically be solved is greatly expanded. Reinforcement learning methods do not need explicit input-output pairs for instruction, unlike supervised learning. By integrating dynamic programming with neural networks, many are hopeful that it can eventually address groups of problems previously unsolvable.

4.1 Problems faced during project

1. Using R language and RStudio for the first time was quite a challenge for us
2. Trying to immerse ourselves into looking for proper response variables before using any random ones
3. Cleaning of data and code as we weren't really used to submitting code that looked perfect on the eye.
4. Factoring out required data frames and understanding the use of PCAs and other relevant documentation of the functions involved in using it.
5. Writing a technical report for the first time.

4.2 Member Contributions

- Sehajvir Singh Pannu – Report related to Model training and Anomaly Detection and technical essay
- Gursmeep Singh Syan - Report related to correlation matrix and HMM and presentation slides
- Roshan Kakadiya – Related to PCA , contribution to slides and technical essay

4.3 Conclusion

We have a clear grasp of what deep learning is and how it works. We have also learned new a new language in R to analyse data. Application of the techniques have helped us understand the frailties of this data and how this data can be used to see things whcich we really cant see without using such techniques.

Machine Learning and AI goes hand in hand when talking about cybersecurity threat analysis. This facet of computer science is going to be crucial in the upcoming years as it creates a whole new realm of how we are making machines do the work for us where we simply study the analysis of such raw data and make decisions based on it.

References:

- https://arxiv.org/pdf/1906.05799.pdf CMPT318
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7307098
- https://ieeexplore.ieee.org/document/5958263
- https://link.springer.com/chapter/10.1007/978-3-642-35197-6_29
- https://www.researchgate.net/profile/Kamalakanta_Sethi/publication/337727475_A_context-aware_robust_intrusion_detection_system_a_reinforcement_learning-based_approach/links/5e202573299bf1e1fab4f9da/A-context-aware-robust-intrusion-detection-system-a-reinforcement-learning-based-approach.pdf
- https://towardsdatascience.com/support-vector-machine-python-example-d67d9b63f1c8
- https://ieeexplore.ieee.org/document/8294288