UNIVERSITY OF WESTERN AUSTRALIA

School of Computer Science and Software Engineering

Thesis Proposal

Selecting Useful Features to Evaluate the Security of Smart Grids

Martin Porebski, 21498791

12 April 2019

Supervisors: Mark Reynolds, Jin Hong

Contents

1. Introduction

1.1 Smart Grids

The distribution of electricity is fundamental to the modern society. The current, traditional approach is a centralised system with a main generator and a static grid [13, 22]. This one-way system has major shortcomings as it is unable to diversify its generation sources or adapt to load changes. This makes the grid inflexible and challenging to upgrade in the future which results in an expensive to maintain infrastructure that is prone to blackouts [13].

Smart Grids will revolutionise the distribution of electricity as they address those issues through an application of smart technology. They utilise a two-way flow of information between the end-users and the grid though the networks of measurement and control devices. Data sharing enables for an automated system which will result in better, real-time control as well as an integration of decentralised generators that can include new sources of energy. The decentralised structure will allow quick blackout restoration and on demand response, while the automation will lower the running costs [13, 22, 32].

Smart Grids are cyber-physical systems that combine electrical and computational devices. The network on which the traffic flows can be separated into three types: HAN (home), NAN (neighbourhood) and WAN (wider area) [2, 13]. To secure the information flow, a number of passive techniques is applied, including secure protocols, encryption and authentication algorithms [13]. However, the network requires an intrusion detection system (IDS) that will detect any suspicious activity such as intrusion attacks, eavesdropping or data manipulation [12, 27].

1.2 Motivation

Security is an essential component in the design of Smart Grids because of the significant impact they have on the everyday life. Power outages costed South Australian

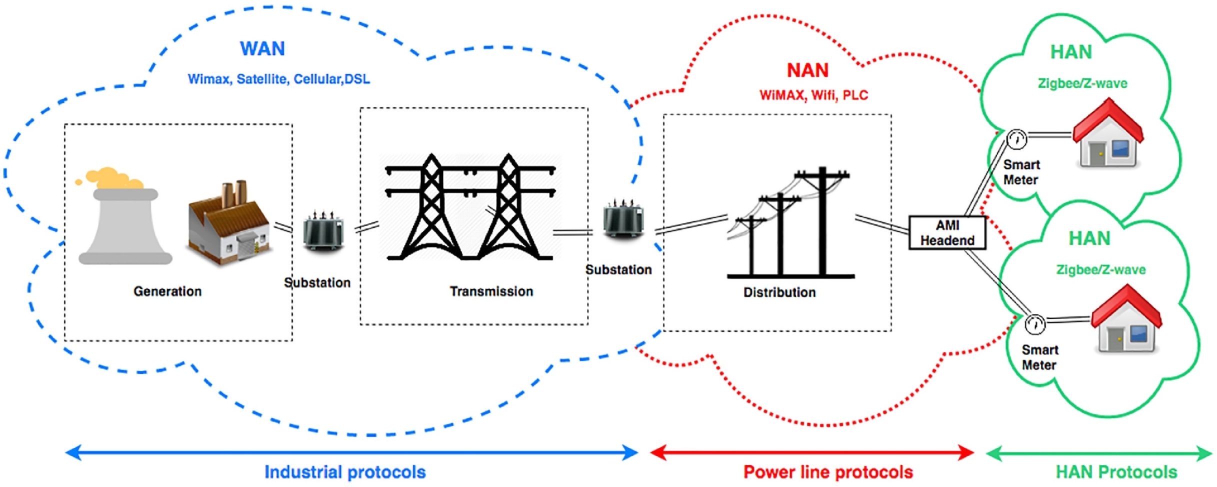

Figure 1.1: Smart Grid Architecture [13]

businesses over $360 million in 2016 alone [17]. Similarly, blackouts cost the U.S. economy an estimated $80 billion every year [13, 14]. Hence, the decentralised Smart Grids will allow a more reliable delivery of electricity, however, there have been multiple threats identified to their security. In 2013, there have been more than 150 cyber attacks on the energy sector alone [3, 14]. Since 2010, malware attacks such as Stuxnet, Duqu, Red October and Black Energy were determined to be an effective way to compromise the grid [22]. In particular, a derivative of Black Energy named Diskali successfully took down the Ukrainian power grid at the end of 2015 which affected over 225 thousand people [5, 22]. Hence, a successful cyber attack on a Smart Grid will result in significant social and financial consequences. The research into the security of the grids is aligned with the policies of Australia's Department of Treasury that overlooks the projects in the energy sector.

2. Problem Identification

2.1 Smart Grid Security

The reliance of the Smart Grids on networking technology, exposed them to the new types of threats. Each new smart device on the grid is an access point that can be exploited. The most recent attacks on the power grids such as Black Energy or Stuxnet have demonstrated the current trend of sophisticated campaigns that exploit vulnerabilities on multiple layers of the system [11, 13, 22].

Based on the standards assessment from the National Institute of Standards and Technology [2], a security framework for a Smart Grid can be identified as [13, 19]:

- Confidentiality - Smart Grids introduce the flow of user data such as metering usage, billing and meter control. As a result, this information needs to remain private, otherwise it could be manipulated or used for malicious purposes.
- Availability - reliable access to the data needs to be maintained on a Smart Grid. A loss of information will affect the control system of the network and may result in a disruption of the distribution.
- Integrity - the flow of information on a Smart Grid is protected from an unauthorised modification or destruction of the data. Authenticity and non-repudiation of the information needs to be confirmed. For example, modification of the data can result in a power theft as one customer's usage can be attributed to another.
- Accountability - the tractability of the system (every action performed by person, organisation or device) needs to be recorded and protected. Those records can be used in consumer or legal disputes, however, if the Smart Grid is compromised, this information will become unreliable.

2.2 Machine Learning for Cyber Security

Some of the approaches to the security threats to Smart Grids are effectively being addressed with Machine Learning (ML). In particular, ML-based approaches are effec-

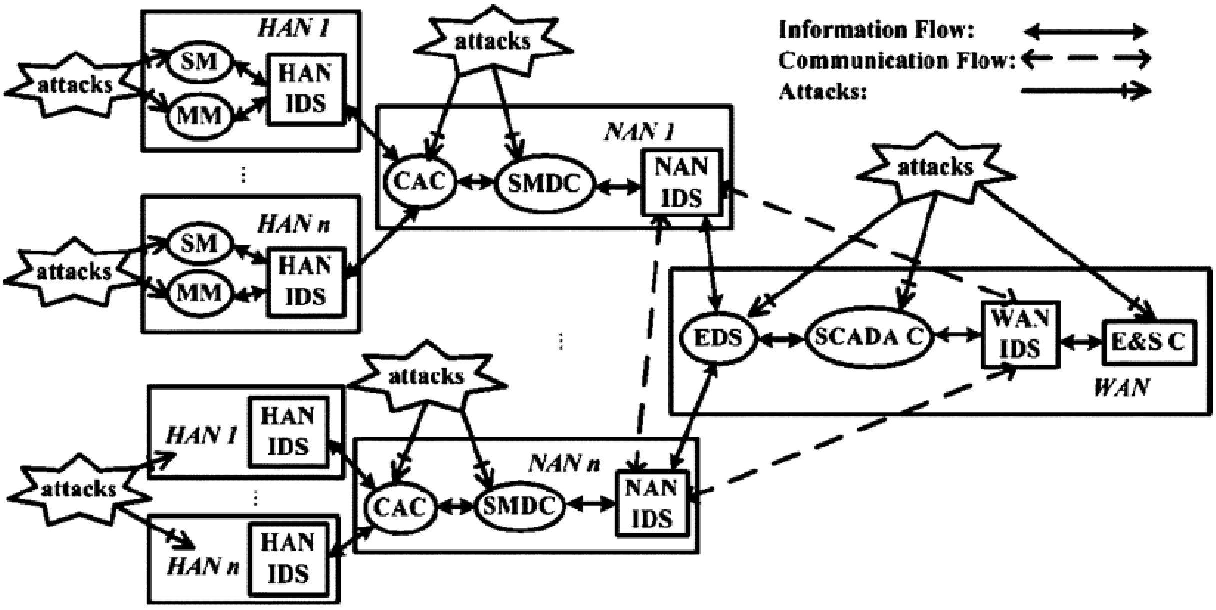

Figure 2.1: Smart Grid Network Architecture [12]

tive in learning the pattern of regular traffic and detecting anomalies [27]. For example, deep neural-networks, artificial neural-networks and state vector machines were used to detect false data injection into the network [7, 32]. Hence, we can utilise them in Smart Grids which generate a large quantity of data from millions of combinations of devices and users. Unfortunately, due to the heterogeneous nature of the network and its scale, the dimensionality of the features and their selection becomes a major issue [12]. In order to improve the performance and correctness of possible ML implementations, features that contribute most to the accuracy need to be selected.

This project will identify new features for improving the security of Smart Grids (SG) using ML techniques. Various feature selection methods will be identified and compared with respect to their accuracy when used in terms of SG security. The performance and accuracy of the existing models will be evaluated using the newly identified features, taking intrusion attacks on SGs as an example.

3. Literature Review

3.1 Attacks on Smart Grids

The current trend in research on the attacks on Smart Grids focuses on general intrusion [12, 24, 27], false data injection (FDI) [6, 7, 32] and data farming attacks (DFA) [30]. The proposed solution involves an Intrusion Detection System (IDS) which passively monitors the traffic on the network and detects malicious activity [27]. IDS is trained with known data to determine the pattern of the regular information flow and detect anomalies in it. Overall, the most successful solutions address a particular network component. State Vector Machines (SVM) with different types of kernels and Mutual Information (SVM MI) selections, Artificial Neural Networks (ANN) and Deep Neural Networks (DNN) proved to be the most reliable anomaly detectors in the Smart Grids. The models are evaluated under [21]:

- General accuracy of detection.
- Recall - ability to identify all of the relevant samples (attacks).
- Precision - ability to identify only the relevant samples (attacks).

Table 3.1 provides a result summary of the most accurate results.

3.2 Machine Learning in Smart Grid Security

3.2.1 False Data Injection (FDI)

FDI is an integrity attack at the physical layer of the Smart Grid [32]. It is considered to be a significant threat to the supervisory (SCADA) systems that are responsible for reliable operation of the grid [6]. It involves modification of the data flowing on the network to compromise state estimations or raw measurements from sensors and meters. FDI can target energy demand, supply, grid-network states and electricity pricing. Hence, it can originate from customers within the grid aiming to reduce their bills, however, organisations or countries may also target their opponents to cause energy disruptions that will lead to considerable financial loses [6, 32].

ML	DFI	FDI	General Intrusion
SVM	A: 95% [30]	A: 75% [32] Linear Kernel [7] P: 95-99% R: 95% Gauss Kernel [7] P: 95-99% R: 75-90%	A: 90% (overall) [27]
SVM MI			A: 76.2% (overall) [27]
k-NN		P: 90-95% R: 80-95% [7]	
ANN		A: 90% [32]	A: 97.6% (normal) A: 45% (other) [27]
DNN		A: 96.2% [32]	

Table 3.1: Attack Detection in Smart Grids. A=Accuracy, P=Precision, R=Recall.

Several papers have proposed various methods that utilise machine learning to generalise the flow of the regular traffic and the detection of the FDI attacks. Ozay et al. [7] explored multiple supervised learning approaches. In addition to evaluating their accuracy, the paper introduced performance as a key metric to be considered in the context of Smart Grids due to their user-demand oriented nature. Perceptron demonstrated the poorest accuracy due to its linear nature. k-Nearest Neighbour (k-NN) was determined to be the most optimal in small scale environments as large dimensionality resulted in poor performance due to the intensive Euclidean distance calculations between samples. SVM performed best in large scale environments (preferable as SGs are large) using the Gaussian kernel to classify the data. Furthermore, SVM was determined to be more successful in detecting the FDI as well as other types of intrusions than the ANN in [27] and [12].

Similarly, a deep learning framework was applied to detect FDI in real-time in [32]. The traffic first passes through a State Vector Estimation which approximates the state of the system from average-case measurements. The residual between estimated and observed data is compared against a fixed threshold to determine a simple data injection. Variations of this approach were used in [6, 8, 9]. However, in [32] it was used as a quality estimator. If above a predetermined threshold, the data is evaluated in a deep neural-network. Each layer of the DNN contains feature detectors allowing it to approximate the higher-order structure of the regular traffic flow on the network. The model incorporates a network's topology, the power measurements from sensors (traffic), energy equations related to the data flow and the associated measurement errors. This allows it to recognise patterns in the temporal features. After the initial learning, the deployed model identifies potential FDIs in parallel to being continuously trained on previous traffic flow. This allows the model to be flexible and stay up-to-date with the network trends. It achieves 95.89% true positive detection and 3.57% false positive with an overall accuracy of 96%. The authors evaluated the accuracy of ANN and SVM on the same data to be below 90% and determined it as being more prone to noise.

3.2.2 Data Farming Attack (DFA)

DFA on Smart Grids targets the information availability and integrity to compromise the operation of the grid [30]. The attacker modifies valid information in the Man-In-The-Middle manner, between the genuine sender and receiver. The attack imperils filters that identify and remove any potentially harmful data (Bad Data Identification and Removal, BDIR). Hence, they result in an incorrect state estimation which is essential for a correct control and operation of the grid [13, 30].

Jiao et al. [30] applied SVM to successfully detect DFA. They found that using SVM proved to be more suitable than neural networks. This is because they had a unique solution due to their convex optimality as opposed to NN, which achieved local minima on each data set [30]. Furthermore, applying the classification kernel performs non-linear transformations which require no assumptions to be made about the data. The trained model achieved the accuracy of over 95%, with a recall of nearly 100%.

3.2.3 Other Intrusion Attacks

ANN and SVM were successfully applied to detect different types of intrusions in the Smart Grids. In [12] SVM was demonstrated to be more appropriate due to its higher accuracy of 0.67% false positive rate and 2.15% false negative rate as well as the most optimal performance across all networks (HAN, NAN, WAN). It was noted that high dimensionality was a significant issue during the feature selection and training phases [12, 27]. Hyper-planes were used to separate and map the diverse data. The classification was achieved with a one-against-one approach that considers one category and combines the remaining classes into one [20]. In [27] the researchers applied mutual information to reduce the dimensionality of the input features. This was based on a similar approach that detected intrusions using ANN in [24]. The tested types of attacks included: normal, exploit, DOS, fuzzer, backdoor, generic and worms. SVM outperformed ANN in detection in all of the categories with an exception of normal where they achieved 93.4% and 97.6% respectively. Overall, SVM had a 76% accuracy, which increased from 76% after applying mutual information method to select valuable features [27].

3.3 Feature Selection & Sensitivity Analysis

Feature selection and sensitivity analysis aim to reduce input space of a learning model and increase its accuracy. Overall, feature selection algorithms isolate attributes that overlap the least with other variables and have high discriminatory power (contribute the most to the training of a model) [25]. The common examples of this are: Principal Component Analysis (PCA), Correlation Feature Selection (CFS) and minimum-redundancy-maximum-relevance (mRMR) [4, 33]. These algorithms can be classified into:

- Filters - omit all the features which are not able to satisfy specified criteria, regardless of the model.
- Wrappers - encapsulates a model to evaluate each selected attribute and delete the irrelevant features.
- Embedded - hybrid of filter and wrapper which includes the process into the training of a model.

The dataset, model and context of the application will influence the selection of features [4, 25]. Hence, the feature selection will strongly depend on the topology of a Smart Grid, its network, the type of attack and the corresponding attributes. For example, [4] classified features in the specific context of botnet attacks on networks based on: protocol, duration, flow size, source and destination ports and IP addresses. The variable importance can be categorised into [18, 25]:

- Predictive importance – investigating the change (increase) in the generalization error when a specific input is discarded.
- Causal importance – manipulating specific input values to investigate how much the outputs will change.
- Marginal importance - considering each input in isolation.

PCA has been successfully applied to aid the detection of intrusion attacks in networks [1, 29, 34]. The approach is able to determine the dominant patterns and extract the most crucial features [31]. However, it is not effective in real-life networks due to its objective function using squared G-norm which is prone to outliers that will result from the noise present in Smart Grids [33]. Modified PCA in [33] achieves a better detection accuracy and higher performance in intrusion detection. This was accomplished by adding a calculation of mean into the feature extraction and using a QR decomposition. Similar to PCA is independent component analysis (ICA) that identifies uncorrelated data based on statistically independent combinations of attributes [25], however, it suffers from the same drawbacks.

Mutual Information is a filter approach that aims at detecting how much the presence or absence of a feature contributes to the classification accuracy [23]. Previously mentioned SVM and ANN [24, 27] were applied in the Smart Grid context to boost the correctness and performance of the models. Multidimensional interaction information (MII) is an improvement that incorporates higher order feature interaction though construing a graph and measuring the most dominant clusters [35].

4. Methodology

4.1 Framework

Overall, the purpose of this project is to optimise the existing detection models through improving their input space and conducting feature selection. The steps for the experiment are (figure 4.1):

1. Collect data - initially, all the relevant resources will have to be gathered. The network and attack data will have to be downloaded from possible sources as outlined in section 4.2. Further research into any additional sources of information might be required.

2. Pre-processing - the raw data will have to be cleaned and evaluated. Smart Grid and network topology will have to be defined. Any relevant components such as network protocols will have to be identified. It is also essential to develop an understating of the information contained within these datasets (features and their significance).

3. Define attack strategy - formulate an attack definition and purpose. Model an attack strategy. This will be based on the research conducted in section 3.

4. Synthetic generation - additional data will be created from an emulated Smart Grid to expand the datasets or simulate attack data (if required).

5. Define optimality criteria for the accuracy and performance of the detection models based on their input features. This will aim to improve the outcomes of the models implemented in the papers outlined in section 3.0.

6. Machine learning - design and train sample models to detect attacks defined in step 3.

7. Output evaluation - assess the results of the trained models.

8. Feature selection - this will include reduction of input dimensionality along with feature analysis and evaluation (see section 4.3). Repeat from step 6 until satisfied with the results.

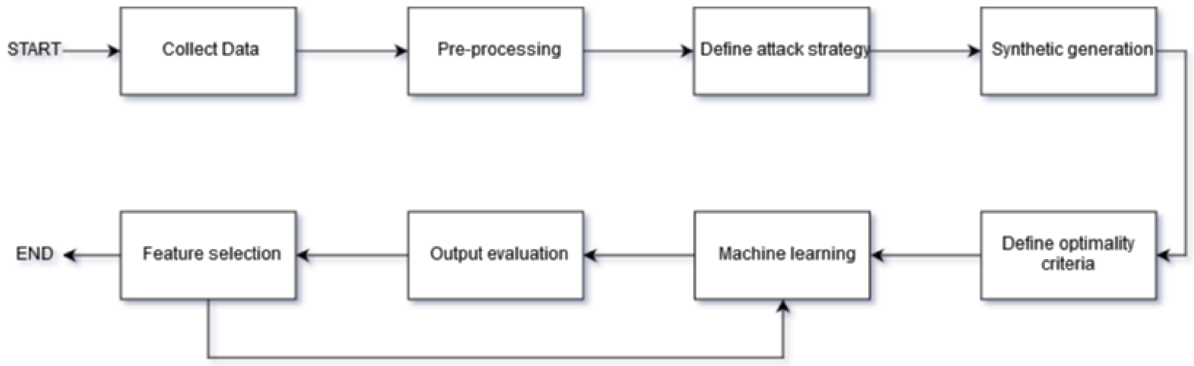

Figure 4.1: Experimental Pipeline

Section 5.2 contains a more detailed task breakdown.

4.2 Raw & Synthetic Data

The feature selection in the context of Smart Grids will depend on the quality of the available training data. The datasets are required to reflect the relevant communication protocols as well as topology of the networks and their heterogeneous nature [11, 26]. In addition to the regular traffic, the data needs to capture intrusion attacks within this context.

Potential sources of data have been identified from current research. KDD-Cup-99 is widely used in anomaly detection due to the large number of records. NSL-KDD is an improved variance which contains over 126 thousand samples of 41 features and 22 different attacks [12, 27]. Similarly, DARPA 1998 and ADFA-LD datasets are used in [27]. The intrusion dataset contains information about nine separate attacks with 44 different features [16, 27]. The data about regular traffic on Smart Grids is also available from a Smart City trail in Australia [15] and from UMass [28]. The intrusion attacks on the industrial control systems (relevant to Smart Grids) was published in [10]. Furthermore, the other authors identified in section 3 can be contacted to request their training data and inquire about their feature selection or pre-processing measures.

Additionally, more data will be synthetically generated based on the available resources. Finding more real-life datasets might be difficult due to the novelty of Smart Grids or the security concerns [11, 26]. Hence, the available data can be enhanced with a synthetic generation. Melody [11] created a framework which emulates large

Smart Grid networks and generates traffic. Furthermore, the authors defined an attack model and generated the corresponding, malicious traffic. When contacted, they provided their dataset and the tool used to generate their data.

4.3 Feature Selection

The previously outlined dimensionality reducing algorithms such as PCA, ICA, MII will be evaluated. Furthermore, multiple variable-sensitivity strategies are to be investigated [11, 18, 25]:

- Exhaustive search - assess all combinations of input features against defined output criteria. This method is computationally expensive with large input spaces.
- Forward selection - incrementally pick variables that optimise model's performance. Prone to getting stuck in local optimum [18].
- Step-wise selection - an extension of forward selection in which if a feature at later iterations is determined to be sub-optimal, it will be deleted.
- Backward elimination - starting with all features, incrementally remove variables with low impact (significance).
- Heuristic search - search the input space to find the optimal set of features through the evaluation of random and predetermined combinations of variables [25].

5. Project Management

5.1 Resources

A powerful enough machine will be required to train the detection models and evaluate their results. This machine will need to at least have 8GB of memory (RAM) and a 1GB GPU. Furthermore, the large datasets will require at least 150GB of free space. This will ensure that the training is conducted in a timely fashion.

Python will be used to clean the data, conduct feature selection, train the models and evaluate results. A combination of NumPy and SciPy packages and/or Tenserflow framework will enable efficient coding and processing. These are popular and free packages. Therefore, there is a large community able to provide support.

5.2 Timeline

The Gantt Chart below demonstrates the task break-down and the intended timeline.

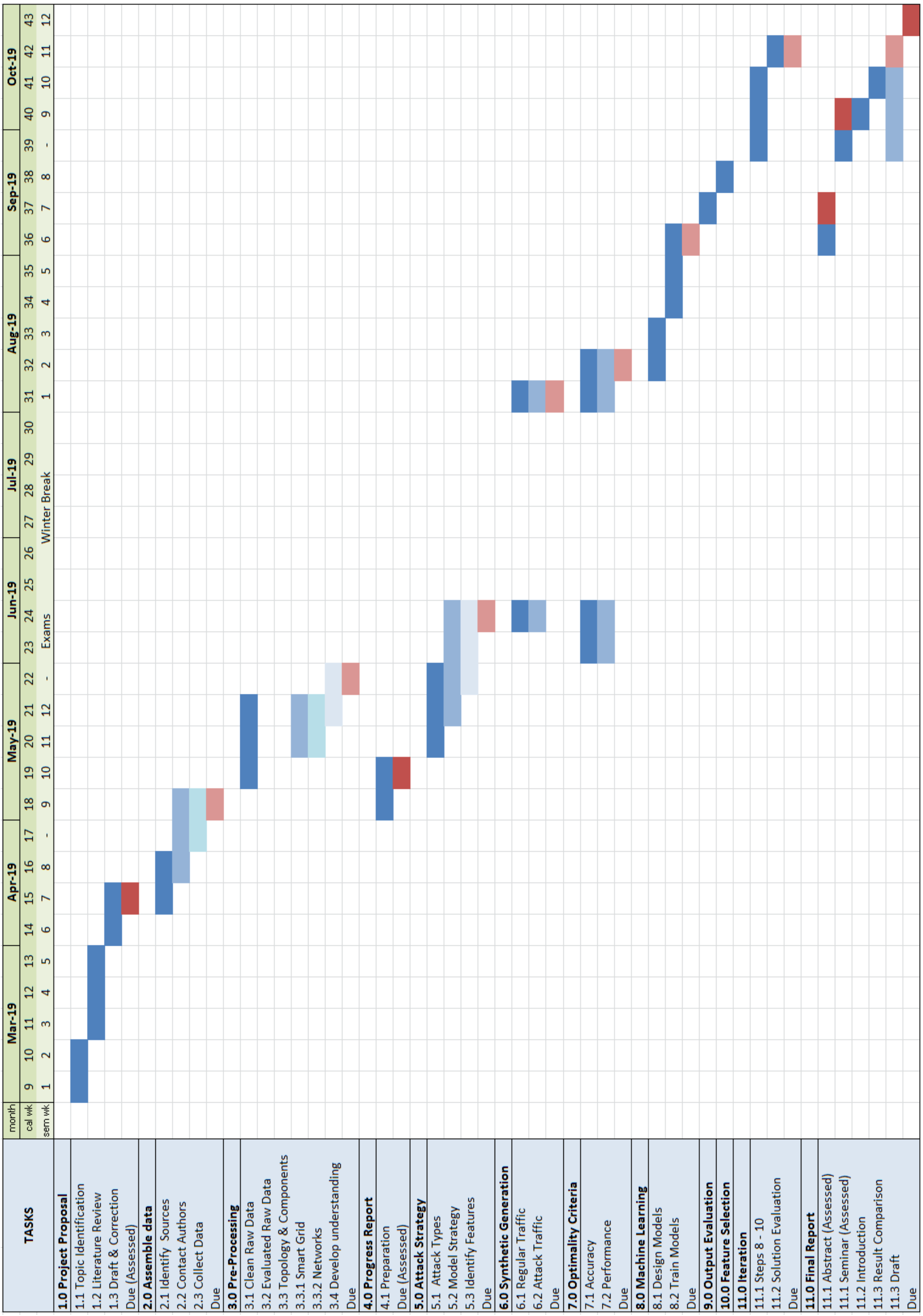

Figure 5.1: Task Break-Down

6 References

[1] C. Callegari et al. "Improving PCA-based anomaly detection by using multiple time scale analysis and Kullback-Leibler divergence". In: *International Journal of Communication Systems* 27.10 (2012), pp. 1731–1751. DOI: 10.1002/dac.2432.

[2] C. Greer et al. "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0". In: (2014). DOI: 10.6028/nist.sp.1108r3.

[3] D. Ding et al. "A survey on security control and attack detection for industrial cyber-physical systems". In: *Neurocomputing* 275 (2018), pp. 1674–1683. ISSN: 0925-2312. DOI: https://doi.org/10.1016/j.neucom.2017.10.009. URL: http://www.sciencedirect.com/science/article/pii/S0925231217316351.

[4] E. B. Beigi et al. "Towards effective feature selection in machine learning-based botnet detection approaches". In: *2014 IEEE Conference on Communications and Network Security* (2014). DOI: 10.1109/cns.2014.6997492.

[5] G. Liang et al. "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks". In: *IEEE Transactions on Power Systems* 32.4 (2017), pp. 3317–3318. DOI: 10.1109/tpwrs.2016.2631891.

[6] Liu et al. "False Data Injection Attacks Against State Estimation in Electric Power Grids". In: *ACM Trans. Inf. Syst. Secur.* 14.1 (June 2011), 13:1–13:33. ISSN: 1094-9224. DOI: 10.1145/1952982.1952995. URL: http://doi.acm.org/10.1145/1952982.1952995.

[7] M. Ozay et al. "Machine Learning Methods for Attack Detection in the Smart Grid". In: *IEEE Transactions on Neural Networks and Learning Systems* 27.8 (Aug. 2016), pp. 1773–1786. ISSN: 2162-237X. DOI: 10.1109/TNNLS.2015.2404803.

[8] M. Ozay et al. "Sparse Attack Construction and State Estimation in the Smart Grid: Centralized and Distributed Models". In: *IEEE Journal on Selected Areas in Communications* 31.7 (July 2013), pp. 1306–1318. ISSN: 0733-8716. DOI: 10.1109/JSAC.2013.130713.

[9] O. Kosut et al. “Malicious Data Attacks on the Smart Grid”. In: *IEEE Transactions on Smart Grid* 2.4 (Dec. 2011), pp. 645–658. ISSN: 1949-3053. DOI: 10.1109/TSG.2011.2163807.

[10] U. Adhikari et al. *Industrial Control System (ICS) Cyber Attack Datasets*. https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets. 2014. (accessed: 01.04.2019).

[11] V. Babu et al. “Melody: Synthesized datasets for evaluating intrusion detection systems for the smart grid”. In: *2017 Winter Simulation Conference (WSC)*. Dec. 2017, pp. 1061–1072. DOI: 10.1109/WSC.2017.8247855.

[12] Y. Zhang et al. “Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids”. In: *IEEE Transactions on Smart Grid* 2.4 (Dec. 2011), pp. 796–808. ISSN: 1949-3053. DOI: 10.1109/TSG.2011.2159818.

[13] Z. Elmrabet et al. “Cyber-security in smart grid: Survey and challenges”. In: *Computers & Electrical Engineering* 67 (2018), pp. 469–482. ISSN: 0045-7906. DOI: https://doi.org/10.1016/j.compeleceng.2018.01.015. URL: http://www.sciencedirect.com/science/article/pii/S0045790617313423.

[14] C. Bajracharya D. B. Rawat. “Detection of False Data Injection Attacks in Smart Grid Communication Systems”. In: *IEEE Signal Processing Letters* 22.10 (Oct. 2015), pp. 1652–1656. ISSN: 1070-9908. DOI: 10.1109/LSP.2015.2421935.

[15] Australian Government Department of the Environment and Energy. *Smart-Grid Smart-City Customer Trial Data*. https://data.gov.au/dataset/ds-dga-4e21dea3-9b87-4610-94c7-15a8a77907ef/details. Sept. 2015. (accessed: 01.04.2019).

[16] J. Hu G. Creech. “Generation of a new IDS test dataset: Time to retire the KDD collection”. In: *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. Apr. 2013, pp. 4487–4492. DOI: 10.1109/WCNC.2013.6555301.

[17] N. Harmsen. *SA blackout costs revealed with fears of more outages*. Dec. 2016. URL: https://www.abc.net.au/news/2016-12-09/sa-blackout-costs-could-have-been-worse-business-sa-says/8106600. (accessed: 01.04.2019).

[18] A. Elisseeff I. Guyon. "An Introduction to Variable and Feature Selection". In: *J. Mach. Learn. Res.* 3 (Mar. 2003), pp. 1157–1182. ISSN: 1532-4435. URL: http://dl.acm.org/citation.cfm?id=944919.944968.

[19] J. Gao J. Liu Y. Xiao. "Achieving Accountability in Smart Grid". In: *IEEE Systems Journal* 8.2 (June 2014), pp. 493–508. ISSN: 1932-8184. DOI: 10.1109/JSYST.2013.2260697.

[20] R. Sabourin J. Milgram M. Cheriet. ""One Against One" or "One Against All": Which One is Better for Handwriting Recognition with SVMs?" In: (Oct. 2006).

[21] W. Koehrsen. *Beyond Accuracy: Precision and Recall*. Mar. 2018. URL: https://towardsdatascience.com/beyond-accuracy-precision-and-recall-3da06bea9f6c.

[22] R. Leszczyna. "Standards on cyber security assessment of smart grid". In: *International Journal of Critical Infrastructure Protection* 22 (2018), pp. 70–89. ISSN: 1874-5482. DOI: https://doi.org/10.1016/j.ijcip.2018.05.006. URL: http://www.sciencedirect.com/science/article/pii/S1874548216301421.

[23] C. D. Manning. *Introduction to information retrieval*. Cambridge University Press, 2018.

[24] D. Devaraj P. Ganesh Kumar. "Intrusion Detection Using Artificial Neural Network With Reduced Input Features". In: *ICTACT Journal on Soft Computing* 1.1 (2010), pp. 30–36. DOI: 10.21917/ijsc.2010.0005.

[25] H. Maier R. May G. Dandy. "Review of Input Variable Selection Methods for Artificial Neural Networks". In: *Artificial Neural Networks*. Ed. by K. Suzuki. Rijeka: IntechOpen, 2011. Chap. 2. DOI: 10.5772/16004. URL: https://doi.org/10.5772/16004.

[26] V. Paxson R. Sommer. "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection". In: *2010 IEEE Symposium on Security and Privacy*. May 2010, pp. 305–316. DOI: 10.1109/SP.2010.25.

[27] B. Kannapiran R. Vijayanand D. Devaraj. "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid". In: *2017 4th International Conference on Advanced Comput-*

ing and Communication Systems (ICACCS). Jan. 2017, pp. 1–7. DOI: 10.1109/ICACCS.2017.8014590.

[28] UMass. *Smart Data Set for Sustainability*. http://traces.cs.umass.edu/index.php/Smart/Smart. 2014. (accessed: 01.04.2019).

[29] B. Surendiran Vasan K. Keerthi. "Dimensionality reduction using Principal Component Analysis for network intrusion detection". In: *Perspectives in Science* 8 (2016), pp. 510–512. DOI: 10.1016/j.pisc.2016.05.010.

[30] V. O. K. Li W. Jiao. "Support Vector Machine Detection of Data Framing Attack in Smart Grid". In: *2018 IEEE Conference on Communications and Network Security (CNS)*. May 2018, pp. 1–5. DOI: 10.1109/CNS.2018.8433210.

[31] Svante Wold, Kim Esbensen, and Paul Geladi. "Principal component analysis". In: *Chemometrics and Intelligent Laboratory Systems* 2.1 (1987). Proceedings of the Multivariate Statistical Workshop for Geologists and Geochemists, pp. 37–52. ISSN: 0169-7439. DOI: https://doi.org/10.1016/0169-7439(87)80084-9. URL: http://www.sciencedirect.com/science/article/pii/0169743987800849.

[32] J. Wei Y. He G. J. Mendis. "Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism". In: *IEEE Transactions on Smart Grid* 8.5 (Sept. 2017), pp. 2505–2516. ISSN: 1949-3053. DOI: 10.1109/TSG.2017.2703842.

[33] M. Benattou Z. Elkhadir K. Chougdali. "An effective cyber attack detection system based on an improved OMPCA". In: *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. Nov. 2017, pp. 1–6. DOI: 10.1109/WINCOM.2017.8238162.

[34] M. Benattou Z. Elkhadir K. Chougdali. "Intrusion Detection System Using PCA and Kernel PCA Methods". In: *Lecture Notes in Electrical Engineering Proceedings of the Mediterranean Conference on Information & Communication Technologies 2015* (2016), pp. 489–497. DOI: 10.1007/978-3-319-30298-0_50.

[35] E. R. Hancock Z. Zhang. "A Graph-Based Approach to Feature Selection". In: *Graph-Based Representations in Pattern Recognition*. Ed. by Xiaoyi Jiang, Miquel Ferrer, and Andrea Torsello. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 205–214. ISBN: 978-3-642-20844-7.