2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications

# Detecting Intrusive Activity in the Smart Grid Communications Infrastructure using Self-Organizing Maps

Zubair A. Baig, Saif Ahmad, Sadiq M. Sait
Department of Computer Engineering, King Fahd University of Petroleum & Minerals, Saudi Arabia
{zbaig, saifahmad, sadiq}@kfupm.edu.sa

***Abstract*—The Smart Grid Infrastructure (SGI) provides for sustainable, affordable and uninterrupted electricity supply to consumers. The communications infrastructure of the SGI is prone to several malicious attacks identified in the recent past. Customer-specific electricity readings are communicated up the SGI hierarchy from consumer devices to centralized servers through intermediary devices such as smart meters and data concentrators/aggregators. In this paper, we model the attacks against the home area network of the SGI, through definition and generation of routine device behaviors. Any observed deviation from the defined normal profile is labeled as a malicious attack. Subsequently, we propose a Self-Organizing Map (SOM)-based approach towards training and testing of centralized SGI devices to qualify them for identifying anomalies accurately. The proposed scheme is capable of detecting anomalous readings within a consumer's household, with reasonable accuracies**.

***Keywords*—**Smart Grid Communications, Anomaly Detection, Self-Organizing Maps, Intrusion Detection.

## I. Introduction

The Smart Grid Infrastructure (SGI) provides a necessary platform for intelligent processing of all activity associated with power generation, transmission and consumption, through a blend of the strengths of computing, intelligence, and high speed data communication [1]. It provides an enhanced and efficient mechanism for energy consumption management by electricity utility customers. In addition, it facilitates better management at the utility provider level through advanced information delivery mechanisms and timely electricity grid fault diagnosis, for ensuring provisioning of high quality service.

The SGI broadly consists of three types of networks, namely, Home Area Network (HANs), Neighborhood Area Network (NAN), and Wide Area Networks (WAN). Each network is interconnected with other networks, and a complex communication hierarchy thus emerges. While the SGI has become a necessity for efficient operations of the contemporary electricity grids, a plethora of malicious attacks may also be perpetrated against it. The malicious intent of such attacks may be either to diminish average electricity consumption at a consumer's end, so as to gain from menial electricity bills, or to maliciously jack up a consumer's bill for adversely affecting the consumer's confidence in a particular utility provider, invariably affecting its business. Other attacks may intend to cause large-scale disruption of routine SGI operations. The SGI interconnectivity to the Internet opens up many entry points for launching both simple as well as sophisticated malicious attacks. Moreover, interconnected network links are vulnerable to cascading failures, wherein, a single transmission line failure may disrupt several other components of the SGI and cause a grid black-out. [2]

Due to the nature of the SGI, contemporary security solutions may not be directly implementable to protect the grid from the omnipresent threat of malicious attacks.

Through this paper, we contribute in the following three ways. First, we model routine behavior of home area network devices and generate data for a 24-hour period for a typical household, based on device types, and empirical power consumption readings. Second, we merge the *normal* behavior data samples with anomalous device behavior data, to form a dataset. The labeling of data samples is done through the definition of distinct rules. The anomalous data samples are generated based on rules which assume that hoax devices or compromised appliances of a home area network (HAN) are capable of generating malicious electricity utilization data for subsequent delivery to the smart meter, thereby resulting in incorrect electricity usage bill of a client.

Third, we propose the use of Self Organizing Maps (SOM), for data clustering, to facilitate classification of SGI data into either the *normal* class or the *anomalous* class. Considering the unsupervised nature of the SOM algorithm, a segment of the unlabeled dataset is introduced to the $n$ x $n$ SOM at training time. The resulting map at the end of training has nodes with fixed vector values (weights) assigned at training time. The testing of the map was conducted through the introduction of unlabeled data samples, and a study of the accuracy in selection, of the appropriate winning SOM node based on a Euclidean distance comparison between the two weights.

The rest of the paper is organized as follows. Section 2

978-0-7695-5022-0/13 $26.00 © 2013 IEEE
DOI 10.1109/TrustCom.2013.196



IEEE computer society

presents a background on the smart grid architecture and related work on intelligent security for the smart grid. In Section 3, we present the dataset generation mechanism with illustrations of data samples. Section 4 provides details on the SOM workings. We present our simulation results and analysis in Section 5 and conclude the paper in Section 6.

## II. Background

The smart grid infrastructure facilitates enhanced degree of control in terms of service provisioning and customer satisfaction, over the electricity grid so as to provide both producers and consumers of electricity with an intelligent and mutually beneficial platform for sustained electricity grid operations [1]. As with all network infrastructures, there exists a potential threat of malicious attacks to affect the smooth operations of the smart grid infrastructure. As a consequence of such attacks, the profitability of the electricity providers is diminished, and the consumer confidence in the affected providers plummets i.e., affects the reputation index of the utility provider. Several attack scenarios and countermeasures have been proposed in the literature to address the growing numbers of threats against the SGI.

Several intelligent techniques have been proposed for anomaly detection through data classification in the SGI. SGDIDS was proposed as a distributed intrusion detection system for the smart grid, in [3]. The system consists of an analyzing module (AM) placed at each of the three layers of the smart grid hierarchy; Home Area Network (HAN), Neighborhood Area Network (NAN), and the Wide Area Network (WAN). Support vector machines (SVM) and Artificial Immune System (AIS)-based algorithms were used as intelligent techniques for detection and classification of smart grid data. In [4], a scheme based on classification of compressed smart meter readings into normal or anomalous, was proposed. A similar approach was proposed in [5] to handle intrusion threats aimed at the advanced metering infrastructure (AMI). A specification-based intrusion detection system is proposed as part of the scheme. A second approach based on specification IDS to perform real time screening of smart meters to access point traffic was proposed in [6]. To ensure smooth system operations in the presence of malicious meters and the threat of DoS (Denial of Service) attacks, the authors defined a set of four monitoring rules. The formulated rules are tested in a realistic environment and a formal verification of the specifications and monitoring operations is carried out at the application layer.

Self-Organizing Maps (SOMs) are a data visualization and mining technique for clustering similar data within predefined numbers of clusters or nodes [7]. They map higher dimension data into 2-dimensional arrays of SOM nodes or neurons. Neighborhood relationship is established through building a topology-preserving map based on the introduced data samples from the dataset. SOMs have been applied to a wide range of areas ranging from pattern recognition to image analysis as well as intrusion detection. It is an unsupervised learning technique, as the data labels of the dataset samples are not required at training time for placement of data samples within predefined SOM nodes. SOMs are implemented within 2-dimensional planes, with *n* x *n* nodes, initially assigned with random feature vector values.

At several places in the literature, SOMs have been applied for clustering network traffic into normal or anomalous.

In [8], one of the first works on SOMs for intrusion detection was proposed. The proposed scheme, ANDSOM, provided a framework for classifying network traffic based on six dimensions i.e. traffic features. Different classes of traffic; DNS, SMTP, and HTTP, were used for building SOMs. Experiments were conducted to test the scheme's effectiveness in network traffic classification.

In [9], an integrated SOM-*k* means clustering approach is proposed for refining the network traffic coarsely through the use of a SOM, and subsequent fine refining through k-means clustering. In [10], a SOM is introduced to identify buffer overflow attacks in a network. Although, reasonable accuracies in attack detection were reported, a long delay in map training was advised as being a disadvantage of using SOMs for intrusion detection. In [11], Radial Basis Functions (RBFs) were used for intrusion detection. The training of the hidden RBF layers was performed through the use of SOMs. It is claimed by the authors that such an approach will boost the effectiveness in attack detection. The experimental results show improved attack detection accuracies through the use of such an approach. Through our work, we propose the use of SOMs for clustering smart grid into normal and anomalous.

## III. Smart Grid device behavior Dataset

A dataset is modeled based on the operating patterns of home appliances in a typical household network of the smart grid infrastructure. The modeled dataset consists of 108,000 data samples. Each data sample consists of 10 appliances, each of which is represented by three parameters (features). These features are: *device_id, randomly generated energy values appertaining to device operation during a given time frame of a day,* and *a difference category*. In addition, each data sample also consists of a label to classify the data sample as either normal (representing routine home network operations), or anomalous, based on the extremity in the readings (too high or too low), when observed collectively.

Table 2 highlights the normal energy consumption in Kwh for devices listed in Table 1. The formula for estimating energy consumption is provided in Equation 1.

$$(\text{Wattage} \times \text{Hours of Operation Per Day}) \div 1000 = \text{Daily Energy Consumption (kWh)} \quad (1)$$

It may be noted that not all appliances/devices are active during all time frames of a day. Therefore, we intuitively describe a combination of devices that are simultaneously active during any given time interval of a particular day. The overall energy consumption during an interval is taken as the aggregated sum of energy consumed by all active devices.

Random values are generated for each device identified as being active during a time interval. An inactive device is given an energy feature value of '0' which indicates a *don't care*, and this value is ignored during determination of the sample class.

The randomly generated energy values are then compared with the estimated normal energy consumption values in Table 2 and a label is assigned to each device. The label assigned may be extreme, marginal or medium, based on the difference between the two energy values (expected and actual):

- Marginal, if the difference is ≤ 15%,
- Medium, if difference is between 15% - 35%, and
- Extreme, if the difference is ≥ 35%.

This criterion is applied to all dataset samples.

A device is known to behave normally if it is labeled as either marginal or medium in the previous step. As such, several instances of the dataset were generated with varying percentages of devices used for defining a particular dataset sample. A total of 5 datasets were thus generated based on the criteria for labeling the dataset samples. For example, one dataset that was used in our experiments had samples labeled as normal if 25% (4 out of 10) devices exhibited normal energy values, and was labeled as an attack instance otherwise. Table 3 highlights the distribution of normal and attack instances in the dataset variants used for our simulations.

It can be concluded from the above statistics that most datasets are imbalanced in favor of either class. This implies that the identification accuracy of the model will be affected since the learning algorithm will encounter more samples from the dominant class of the dataset in question. For instance, the 65% dataset is heavily biased towards the attack class with nearly twice as many attack rows as the normal rows. In order to minimize the effect of the bias, we select the 55% dataset as it has the lowest difference between the two classes.

TABLE I
POWER RATINGS FOR COMMON HOUSEHOLD DEVICES

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

## IV. SELF-ORGANIZING MAPS FOR INTRUSION DETECTION

The datasets generated in the previous section were introduced to a Self Organizing Map for training. The resulting map provides a clustered visualization of data, through established node relationships.

Training begins on a SOM whose nodes have already been assigned random values for their respective local vectors (weights). The SOM training algorithm operates iteratively, with samples introduced to the SOM one at a time, and the best matching node of the SOM selected as a winner, for a given iteration. The length of the input vector is dependent on the number of features that represent the data in question. The training process is iteratively executed, with the winner node selected based on its closest proximity to the incoming data sample, when compared to the proximities of other nodes. Subsequently, all nodes within the neighborhood of the winning node have their respective weights updated so as to closely fit the data sample which led to this particular node's win. The winning node and its neighbors have their respective feature vector values modified based on a predefined formulation. The SOM map settles to a certain 'good fit' state after all iterations (equal to the number of data samples that were introduced), are completed. The resulting map is organized inherently in a way such that nodes with mutual similarities in terms of their respective weights will be clustered close to each other.

We assign meaning to the nodes of the maps through introduction of labels. Post training, the SOM nodes are labeled as being either *normal* or *anomalous*, based on the

TABLE 2
ENERGY CONSUMPTION (KWH) OF HOME APPLIANCES

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

TABLE 3
BASIC DATASET CHARACTERISTICS

| Dataset Type | Normal Rows | Attack Rows |
|---|---|---|
| 25% | 79036 | 28964 |
| 35% | 79017 | 28983 |
| 45% | 76884 | 31116 |
| 55% | 43443 | 64557 |
| 65% | 39834 | 68166 |

majority in the number of samples of each type that are assigned to a particular winning SOM node during training. The testing of the SOM is conducted through the introduction of unlabelled data samples to the SOM, and observation of the class labels of the best matching nodes.

Following are the steps of execution of the SOM training algorithm:

**Step 1:** Construct a weight matrix

**Step 2:** Initialize the weight matrix with randomly selected input vectors

**Step 3:** For each input vector x,

3.1 Compute Euclidean distance between each node's weight vector and the current input vector:

$$Dist = \sqrt{\sum_{i=0}^{n} (V_i - W_i)^2} \qquad (2)$$

3.2 Choose the winner as the neuron c, such that the distance between the input vector and the neuron is smallest.

**Step 4:** Adjust the weights for the winner and all its neighbors: $W(t+1) = W(t) + \theta(t) \cdot L(t) \mid V(t) - W(t) \mid$ where L(t) is the learning rate, and θ(t) is the neighborhood kernel function centered on the winner unit

**Step 5:** Decrease the learning rate and neighborhood size

**Step 6:** Repeat steps (2)-(5) until the convergence criterion is satisfied.

**Algorithm 1:** SOM Training Steps

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

## V. Results and Analysis

### *A. SOM training parameters*

Simulations were performed to test the ability of our proposed approach to accurately classify smart grid data into normal and anomalous. In Table 4, we provide the SOM training phase parameters selected for running the simulations.

### *B. True Positives versus False Positives*

Figs. 1- 5 present a comparison of the true positives and the false positives generated through simulation, for the five varying dataset labels (as elaborated in Section III). It can be observed that varying the size of the SOM map has an effect on the detection rate. It can be concluded from the results obtained that the dataset where 45% of devices in a sample behave normally provides the best true positive rate and this rate is achieved for a map size of 4 x 4. Also it can be noted that for almost all datasets the maximum true positives are reported for the 4x4 map size. For a 25% ratio dataset, the highest detection rate was observed to be 57% at the cost of 49% false positives. For larger map sizes, the false positives were found to outweigh the detection rates. A similar trend was observed for the other datasets tested. For the 25%, 35%, and the 45% datasets, a common trend observed was of having the detection rate of a 5 x 5 map outperforming other map sizes. However, for the 55% and 65% datasets, the trend did not continue, and a consistent detection rate of 40% was observed regardless of map size, for a constant set of false positives of 60% generated.

### *C. True Positives versus False Positives (Fixed Attack to Normal Ratio)*

A second set of experiments were conducted by varying the percentage of attack instances in the training set while maintaining a 50-50 ratio between attack and normal instances within the test set. The number of attack instances within the training set was varied from 20% to 70%. It was observed that the results obtained for all the experiments were identical, as illustrated in Fig. 6. There was a 100% detection rate for the entire test set. However, while all the attack instances are detected as true positives, all the normal instances are detected as false positives. In this experiment, the variation of learning rate had no effect on the final outcome. It can be inferred from these results that the SOM neurons are over-trained with attack instances and hence are unable to detect any of the normal instances in the dataset.

TABLE 4
SOM TRAINING PARAMETERS

| Parameter | Value |
|---|---|
| Initial L(t) | 0.5 |
| SOM Map size (Variable) | 2 x 2 to 10 x 10 |
| L(t) decay function | $L(t) = L_0 \exp^{(-t/\lambda)}$ |
| Training Iterations | 75600 |
| Neighborhood Function | Gaussian |
| Topology | Matrix |

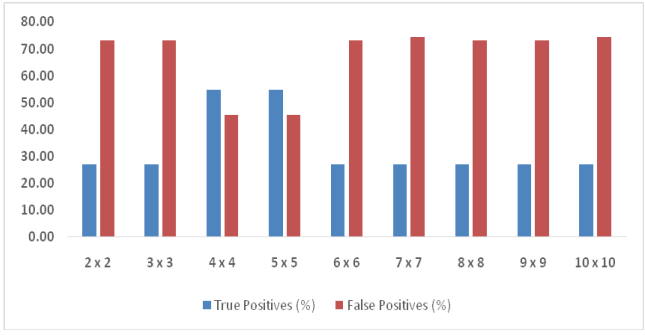


Fig. 1 True Positives and False Positives for a 25% ratio dataset for varying map sizes (ranging from 2x2 to 10x10)

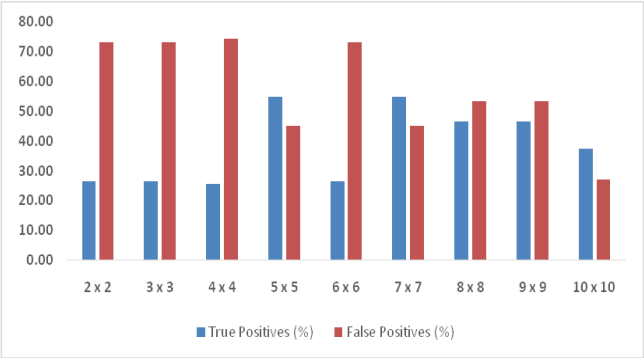


Fig. 2 True Positives and False Positives for a 35% ratio dataset for varying map sizes (ranging from 2x2 to 10x10)

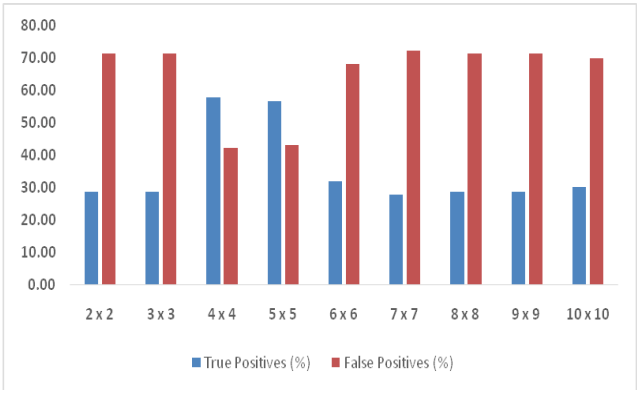


Fig. 3 True Positives and False Positives for a 45% ratio dataset

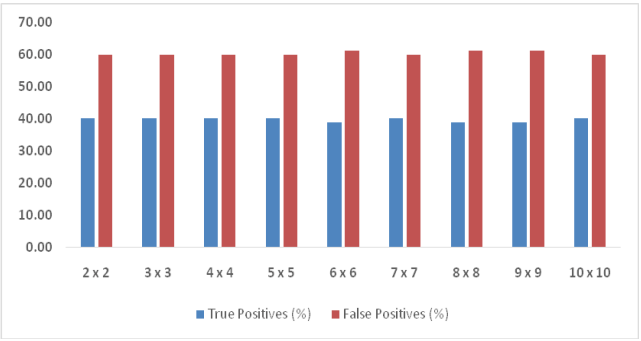


Fig. 4 True Positives and False Positives for a 55% ratio dataset for varying map sizes (ranging from 2x2 to 10x10)

### *D.True Positives versus False Positives For UMass Smart* Home Data Set*

A third set of experiments were conducted on the UMass Smart* Home Data Set [12]. This dataset is composed of a wide variety of environmental and operational data from three real home area networks. We have only considered data from one of the homes in our experiments, namely, Home B. The dataset contains information about home electricity usage parameters such as average household electricity usage every second, as well as electricity usage at each circuit and nearly every plug load, electricity generation data from on-site solar panels and wind turbines, outdoor weather data, temperature and humidity data in indoor rooms, and, finally, data for a range of important binary events, e.g., at wall switches, the HVAC system, doors, and from motion sensors.

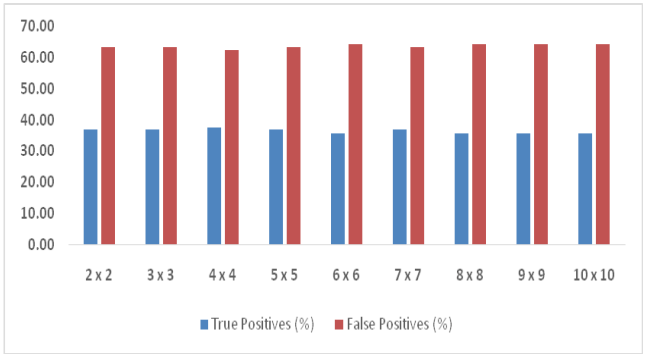


Fig. 5 True Positives and False Positives for a 65% ratio dataset for varying map sizes (ranging from 2x2 to 10x10)

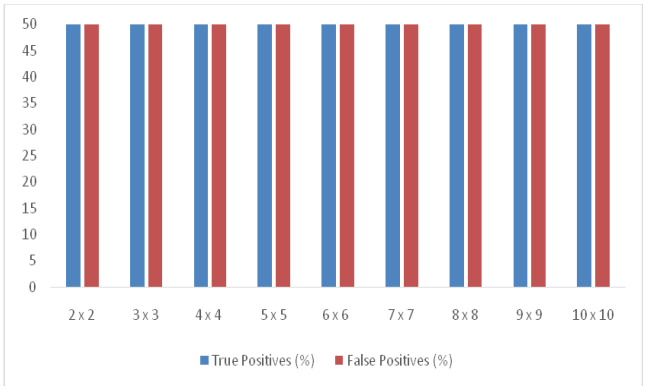


Fig 6 True Positives and False Positives for a 50% ratio dataset for


varying map sizes (ranging from 2x2 to 10x10)

Fig. 7: True Positives and False Positives for a 25% ratio dataset for Smart* dataset

Figs. 7- 8 present a comparison of the true positives and the false positives generated through simulation, for the five varying dataset labels of the Smart* Home dataset, when a

Self-Organizing Map was used for training and testing. A sample split of 70-30% was considered for the simulations, similar to the previous runs. It can be inferred from the obtained results that varying the dataset has negligible effect on detection rates for map sizes of 2x2 and 3x3. Even for a map size 4x4 the detection rate remains similar until the 55% ratio dataset is chosen, where the number of true positives is significantly greater than the false positives. An overall analysis of the results reveals that the dataset in which 55% of the devices are behaving normally provides the highest true positive rate and this rate is achieved at a map size of 8x8. It can be observed that for most datasets the best true positives rates are achieved at large map sizes of 7x7 and above except for the 25% dataset where the best true positive rate is found when a map of size 5x5 is chosen.

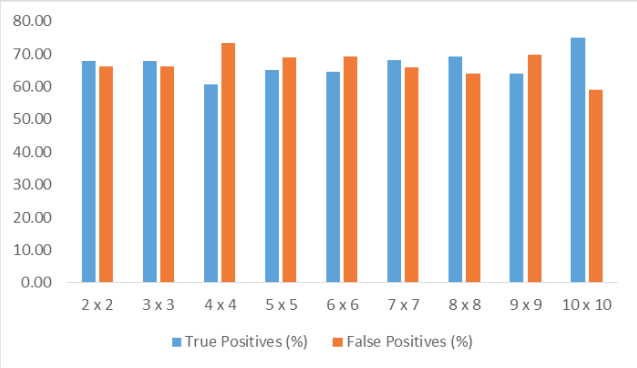


Fig. 8: True Positives and False Positives for a 45% ratio dataset for Smart* dataset for varying map sizes (ranging from 2x2 to 10x10)

The highest true the highest detection rate was observed to be 78% at the cost of 57% false positives. In most cases for larger map sizes, the false positives were found to outweigh the detection rates except for the 35% dataset and 65% dataset.

### *E. Execution Times*

The size of the SOM a direct impact on the delays incurred at time of training. In Fig. 9, an illustration of the execution time for the SOM training for varying map sizes is provided. As may be observed, for map sizes of 5 x 5 and below, the training time is less than 1000 seconds, whereas, for larger map sizes, the time required to train the map for the same dataset is exceedingly high, with 9000 seconds being the peak value observed for a 10 x 10 map.

## VI. Conclusion

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

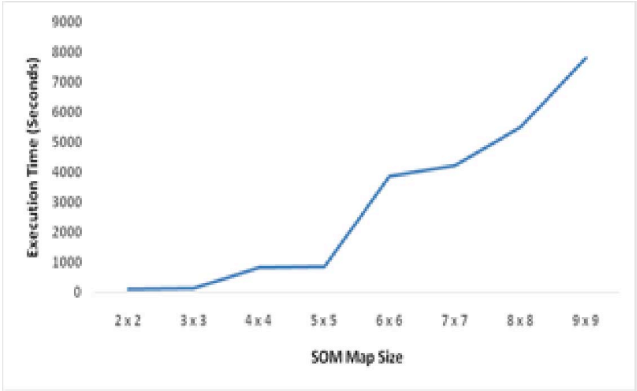


Fig. 9: The Execution Time for Training i.e. Map building of the SOM – for both datasets

## VII. Acknowledgements

The authors wish to thank King Fahd University of Petroleum & Minerals for its continuing research support. This research work was conducted as part of the research project no. NSTIP-11-INF1658-04.

## References

[1] S. Ahmad and Z.Baig, " Fuzzy-based Optimization for Effective Detection of Smart Grid Cyber-Attacks," *International Journal of Smart Grid and Clean Energy*, vol. 1, pp. 15-21, 2012.

[2] Pallotti E, Mangiatordi F. Smart Grid Cyber Security Requirements. *Roma Tre University, Electronics Dept*., 2011.

[3] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Transactions on Smart Grid*, vol. 2, pp. 796 –808, Dec. 2011.

[4] H. Li, R. Mao, L. Lai, and R. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Proc. 1st Smart Grid Communications (Smart-GridComm) Conf.* , Washington, DC, 2010, pp. 114 –119.

[5] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Proc. 1st Smart Grid Communications (Smart-GridComm) Conf.* , Washington, DC, 2010, pp. 350 –355.

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

[7] T. Kohonen, "Self-Organizing Maps," Springer Series in Information Sciences. Berlin, Heidelberg: Springer. 1997.

[8] M. Ramadas. "Detecting Anomalous Network Traffic with Self-Organizing Maps," *Master's thesis*, Ohio University, Mar 2003.

[9] W. Huai-bin, Y. Hong-liang, X. Zhi-jian, and Y. Zheng, "A Clustering Algorithm Use SOM and K-Means in Intrusion Detection", in Proc. Intl Conf on E-Business and E-Government, 2010, pp.1281-1284.

[10] Vivek A Patole, V K Pachghare and Parag Kulkarni. Self Organizing Maps to Build Intrusion Detection System,".*International Journal of Computer Applications* vol. 2, pp. 1–4, Feb. 2010.

[11] Li-Ye Tian and Wei-Peng Liu, "Incremental intrusion detecting method based on SOM/RBF," *in Proc. Intl. Conf. on Machine Learning and Cybernetics (ICMLC)*, 2010, pp.2849-2853.

[12] S. Barker, A. Mishra, D. Irwin, E. Cecchet, P. Shenoy, and J. Albrecht., "Smart*: An Open Data Set and Tools for Enabling Research in Sustainable Homes" in Proc. of the 2012 Workshop on Data Mining Applications in Sustainability, 2012.