IIOAB JOURNAL
ISSN: 0976-3104

ARTICLE

A SECURE DEEP BELIEF NETWORK ARCHITECTURE FOR INTRUSION DETECTION IN SMART GRID HOME AREA NETWORK

Divya M Menon*, N Radhika

Department of Computer Science and Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Amrita University, Coimbatore, INDIA

ABSTRACT

The Deployment of Smart Grid requires consideration of all the security parameters in the entire architecture of Smart Grid. Data Security and Communication Security are the major milestones in security that need to be addressed in the present scenario in Smart Grid. In this paper we model a Deep Belief Network to detect the normal and abnormal behaviors in the traffic pattern of Smart Grid data. Deep belief Network has been deployed to identify the anomalies in the Smart Grid data traffic thereby detecting intrusion .Support Vector Machine has been used for intrusion classification after creating the Deep Belief Network Model. Using SVM model with deep belief networks has helped in reduction of data complexity and also in identifying the core features to be considered for the implementation of Intrusion detection in Smart Grid Model.

KEY WORDS
Smart Grid, Deep Belief Network Intrusion Detection, Home Area Network

Received: 10 October 2016
Accepted: 12 November 2016
Published: 1 Dec 2016

INTRODUCTION

Security is gaining high focus in the Smart Grid deployment in the recent years[1]. New strategies for implementation of security in data communication in the Smart grid network remains an expensive task .Primary issue in security can be override by the detection of third party intruders in the Smart Grid Network. Hence intrusion Detection needs to be tackled at every level of communication in Smart grid before the deployment of Secure Smart Grid[2]. Smart Grid Architecture model contains mainly three phases: Generation, Transmission and Distribution Our work is mainly concentrated in providing communication security in the Distribution end of Smart Grid. Here we analyse the traffic patterns in the Last mile communication at the distribution side. The rate of data traffic at the distribution side is higher when compared to other phases in Smart Grid Architecture Model. Deploying security at this phase poses high challenges due to the massive data traffic. A better analysis of Smart Grid traffic data needs to be done to identify the anomaly and to detect intrusions. Consequently Big Data and Machine Learning solutions need to be considered while working with Smart Grid traffic data. Big Data Analytics and Machine learning has become promising areas while deploying security in major areas of research [3]. Smart Grid traffic has massive data for analysis and hence we need to extract meaningful features from these massive input data for decision making context in identifying the normal and abnormal behaviours. Feature extraction requires efficient methods since these features are used for classification of data as well as for creating prediction model. The Input data from the Smart Grid poses many format variations and large amount of noise. It may also be of greater dimensions which makes it harder to analyse. Deep learning algorithms offer solutions to these analysis of massive Big data [4].

DEEP BELIEF NETWORKS FOR SMART GRID DATA TRAFFIC

In this section we have presented a theoretical background of Deep Belief Networks. Design Architecture of our proposed Deep Belief Networks have been presented here. The key concept in Deep learning algorithms is the extraction of key features from the numerous features in the Big Data which may have both wanted and unwanted elements[5]. Deep Belief Networks generates a small amount of data for classification from unlabeled big data thus making it faster. Since these models are largely motivated from artificial intelligence and neural networks they follow a hierarchical pattern for analysis[6].

A multi layer architecture is deployed in Deep Belief Networks with each layer identifying features and relationships which are beyond immediate neighbours from previous layers. Each layer of DBN is constructed by Restricted Boltzmann Machines(RBM)[7,8]. Restricted Boltzmann machine (RBM) can learn probability distribution from a set of input data. The core block networks of the DBN are Restricted Boltzmann Machines (RBMs),which consists of a visible layer and a hidden layer[9-11]. The visible variables in the layer are described as the features of the input data .RBM uses Contrastive Divergence algorithm to approximate samples of data was proposed by Hinton[12,3].Deep Belief Networks takes as input a matrix representation of data set and identifies patterns which are used to identify relevant features in each layer of the DBN architecture[13,14][16,17].

***Corresponding Author**
Email: divya@jecc.ac.in
Tel.: +91-9495880085

IIOAB JOURNAL
ISSN: 0976-3104

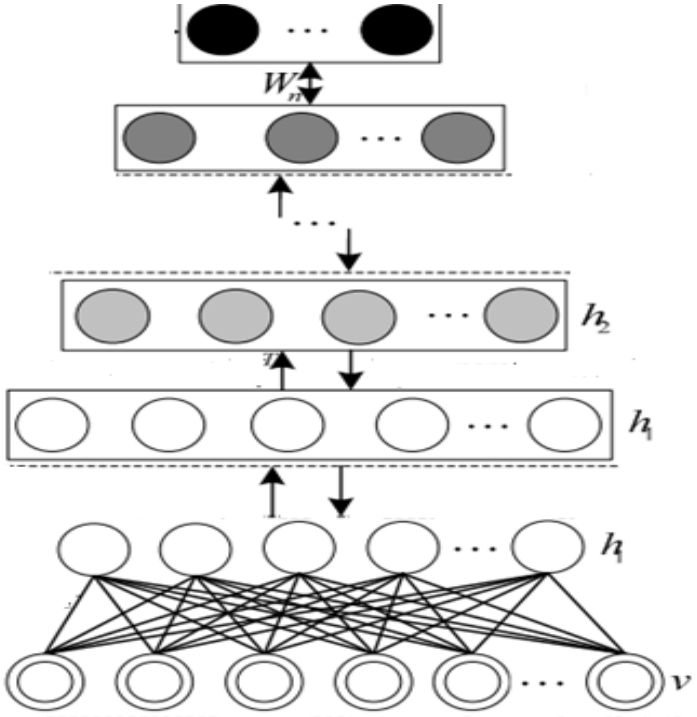

Fig. 1: Deep belief network representation.

RBM consists of a matrix of size m*n having weights W between hidden units h and visible units v , and offsets x,y for the visible units and hidden units respectively.The general Energy representation of RBN is denoted by E(v,h),

$$E(v,h) = -xTv - yTh - vTWh \quad (2.1)$$

By using the Energy function Marginal probability of visible vector is calculated The features having probability less than this marginal probability is removed to extract relevant features.The Marginal Probability of visible vector is the sum of configurations of hidden layers.

$$P(v) = (1/Z) \sum e^{-E(v,h)} \quad (2.2)$$

Here Z represents Partition function.

Algorithm for deep belief network architecture

Procedure for DBN Architecture

D:Data
RBM: Restricted Boltzmann Machine
RV: Set of RBMs
TD: Training Data
TRBM:Train RBM
NFRBM:Not Final RBM
LRBM:Last RBM
MAV: A Boolean variable to identify whether to use Mean Activation Value or not when moving to other values in RBM layers.
QF: A Boolean variable to identify whether or not to query Lh(Hidden layer).

1.Input Data to training data set
2.For all RBM in RV perform
RBM ⟵ TRBM(TD)
until LRBM
3.If (NFRBM) || (LRBM && QF) then
D ⟵ Move(RBM,D,MAV)

IIOAB JOURNAL
ISSN: 0976-3104

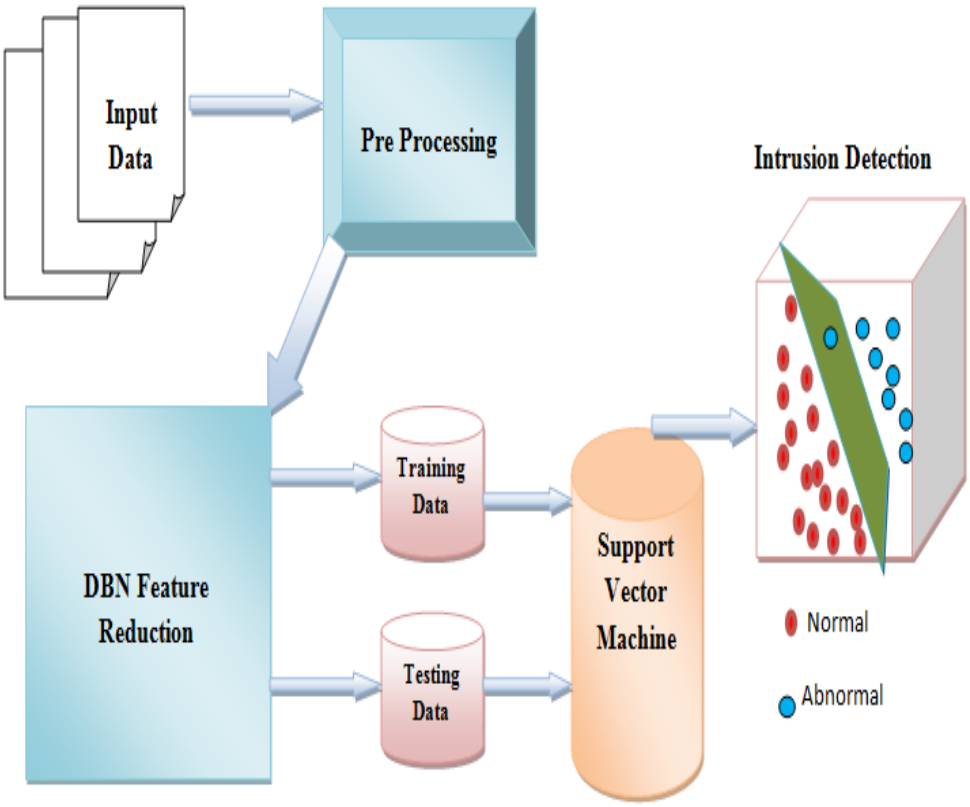

Fig. 2: Intrusion detection architecture model using DBN.

IMPLEMENTATION OF ANOMALY DETECTION USING DEEP BELIEF NETWORKS

Deep Belief Network Learning is semi supervised machine learning algorithm which identifies sudden behavioural changes called anomalies in data behaviour .The steps involved in Intrusion Detection using RBM :

1. Remove Noise from input data.
2. Input N:No of Layers
3. For all Li
   (i)Applying training for the first layer Li of preprocessed data.
   (ii)Input Mean Activations as training data to second layer Li+1.
4. Repeat (3) for N no of layers in ascending order moving through layers in upward direction until layer LN is reached.
5. Apply SVM Classifier for Reduced DBN Data.
6. Calculate threshold value to identify whether data is normal or abnormal cluster centres until no reassigning is needed.

In this paper we use Deep Belief Networks to extract relevant features from the large traffic data in Smart Grid. Input data from traffic is pre-processed to remove noises and unwanted elements. The pre-processed data is fed into Deep Belief Network to reduce the features and to identify important features. The output of DBN will have same number of rows for data set and the number of columns indicating features will be reduced. The output of DBN is given to Support Vector Machine Classifier .SVM classifier identify whether each row in the data set represents a normal or abnormal behaviour based on the training data. We have implemented Deep Belief Networks using R Programming with the help of package deep net. For the purpose of Visualization Weka has been used. [Fig. 3] depicts the graph obtained to demonstrate the normal and abnormal behaviour. The blue points normal data and red points represent abnormal data

IIOAB JOURNAL
ISSN: 0976-3104

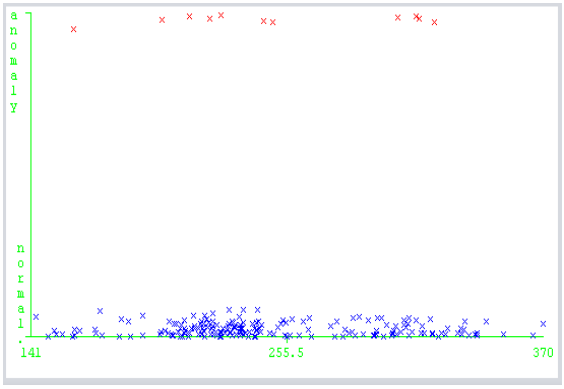

Fig. 3:

Table 1: Evaluation on training set in weka

Sl No	Parameters	Values
1	Total No of Instances	199
2	Correctly Classified Instances	188 - 94.47%
3	Incorrectly Classified Instances	11 - 5.52%
4	Mean Absolute Error	0.1084
5	Root Mean Squared Error	0.2286
6	Time taken to test model on training data	0.01 seconds

Here we have taken 199 instances and the result showed 188 correctly classified instances and 11 incorrectly classified instances.

```
=== Confusion Matrix ===

   a   b   <-- classified as
 188   0 |   a = normal.
  11   0 |   b = anomaly
```

Fig. 4: Confusion matrix of normal and anomaly instances.

[Table 1] shows the evaluation conducted. Mean Absolute Error measures the average errors in a data set[15]. Root Mean Squared Error uses quadratic calculation for determining the average magnitude of error in a data set.Both these values are used together to identify the variations in errors.[Table 2] shows detailed class accuracy for the testing data.TP rate , FP Rate denotes the rate of correctly classified instances and incorrectly classified instances respectively.Precision is calculated by dividing the true instances with the total instances (TP+FP). F-Measure is calculated using the equation, F-Measure = 2 *P*R/(P +R),where P represents Precision and R represents Recall. Receiver operating characteristic (ROC) plots TP rate against FP Rate. PRC represents Precision Recall Curve Area. [Fig. 4] represents the Confusion Matrix which identifies 188 normal instances and 11 anomaly in the data set.

Table 2: Detailed Class Accuracy in Weka

TP Rate (TP)	FP Rate(FP)	Precision(P)	Recall(R)	F-Measure	ROC Area	PRC Area	Class
1.000	1.000	0.945	1.000	0.972	0.500	0.945	Normal

IIOAB JOURNAL
ISSN: 0976-3104

0.000	0.000	0.000	0.000	0.000	0.500	0.055	Anomaly
0.945	0.945	0.893	0.945	0.918	0.500	0.896	Weighted Avg

CONCLUSION

In this paper we have implemented anomaly detection for Smart Grid traffic data using Deep Belief Network algorithm which extracts relevant data from Big Data.A Deep Architecture has been deployed using DBN along with Support Vector Machine Classifier. A stack of Restricted Boltzmnn Machines(RBM) networks are used to deploy DBN . The evaluation has been done in R programming and the anomalies hidden in dataset were identified .Results found for anomaly detection identified all the injected anomalies in the Smart grid traffic.Weka tool has been used to plot graphs to identify anomaly in traffic for better visualization.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Jixuan Zheng; Gao DW, Li Lin. [2013] Smart Meters in Smart Grid: An Overview," IEEE Conference Green Technologies, pp.57,64, 4-5 April.

[2] Alom MZ, Bontupalli V, Taha TM,[2015] Intrusion detection using deep belief networks," 2015 National Aerospace and Electronics Conference (NAECON), Dayton, OH, pp. 339-344.

[3] Gao N, Gao L, Gao Q, Wang H.[2014] An Intrusion Detection Model Based on Deep Belief Networks, 2014 Second International Conference on Advanced Cloud and Big Data (CBD),, Huangshan, pp. 247-252

[4] Chen Z, Liu S, Jiang K, Xu H, Cheng X.[2015] A Data Imputation Method Based on Deep Belief Network, 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, pp. 1238-1243.

[5] Zhang Q, Yang LT, Chen Z.[2016] Privacy Preserving Deep Computation Model on Cloud for Big Data Feature Learning," in IEEE Transactions on Computers, 65(5): 1351-1362.

[6] Seethal K, Divya M Menon, Radhika N.[2015] Design of a Secure Smart Grid Architecture Model using Damgard Jurik Cryptosystem". Research Journal of Applied Sciences, Engineering and Technology, 9(10): 895-901

[7] Divya M, Menon N, Radhika.[2015] Design of a Secure Architecture for Last Mile Communication in Smart Grid Systems", Procedia Technology, 21: 125-131, ISSN 2212-0173.

[8] Hasen Nicanfar, Peyman Talebifard, Amr Alasaad and Victor C. M. Leung, "Enhanced Network Coding to Maintain Privacy in Smart grid Communication",IEEE Trans .Emerging Topics In Computing, 1(2) December 2013.

[9] Sun X, Li C, Xu W, Ren F.[2014] Chinese Microblog Sentiment Classification Based on Deep Belief Nets with Extended Multi-Modality Features, 2014 IEEE International Conference on Data Mining Workshop, Shenzhen, pp. 928-935.

[10] Meiyin Wu, Chen Li.[2015] Image recognition based on deep learning," Chinese Automation Congress (CAC), 2015, Wuhan, pp. 542-546.

[11] Pin-Yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen, [2012] Smart Attacks in Smart grid Communication Networks, IEEE Communications Magazine.

[12] Hecht C, Reichl P, Berge, A, Jung O, Gojmerac I.[2009] Intrusion Detection in IMS: Experiences with a Hollinger Distance-Based Flooding Detector. First International Conference on Evolving Internet, 2009. INTERNET '09, pp.65-70, 23-29

[13] Jianhong, Hu, "Network Intrusion Detection Algorithm Based on Improved Support Vector Machine," in International Conference on Intelligent Transportation, Big Data and Smart City (ICITBS), 2015 , vol., no., pp.523-526, 19-20 Dec. 2015.

[14] Attia M, Sedjelmaci H, Senouci SM, Drive EHA. [2015]A new intrusion detection approach against lethal attacks in the smart grid: temporal and spatial based detections, in Global Information Infrastructure and Networking Symposium (GIIS), 2015, pp.1-3, 28-30

[15] Davoudi A, Chatterjee M.[2015] Product rating prediction using centrality measures in social networks, Sarnoff Symposium, 2015 36th IEEE, Newark,NJ, pp. 94-98.

[16] Arunkumar N, Balaji VS, Ramesh S, Natarajan S. [2012] Automatic detection of epileptic seizures using Independent Component Analysis Algorithm. In Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on (pp. 542-544). IEEE.

[17] Stephygraph LR, Arunkumar N, Venkatraman V. [2015] Wireless mobile robot control through human machine interface using brain signals. In Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 International Conference on (pp. 596-603). IEEE.