ISSN No:-2456-2165

Intrusion Detection in Smart Grid

Anzar Iqbal
M-tech scholar CSE
(Sharda University)
Greater Noida, India

Mohammad ummer chopan
M-tech scholar CSE
(Sharda University)
Greater Noida

Pooja
Associate Professor
(Sharda University)
lGreater Noida, India

Abstract:- The idea of smart grid has extensively changed over the customary power framework into the massive Cyber Physical network that empowers the bidirectional correspondence between the grid administration focuses and the end clients. However, the presentation of such foundation have made the power frameworks significantly more adaptable and productive, with many Smart Devices included, yet additionally builds the danger of security attacks exponentially. The gadgets that are being utilized in smart grid goes about as provisos or more fragile point and give a surface region to intruders for embedding malware. So as to upgrade the security of smart grid different security instruments called intrusion detection systems are utilized, which includes the arrangement of different Intelligent Modules in numerous layers of shrewd network all together defeat the cyber threats. These Intelligent Modules utilize different Classification Algorithms to distinguish and arrange the malicious data and dependent on that perception recognizes whether there is a security assault or not. In this paper we are going to present an approach towards the classification various events (attack or natural) occurring in smart grid for enhancing the security in smart grid and hence prevent them from any sort intrusion that can disrupt normal functioning of smart grid.

Keywords:- *Component, Formatting, Style, Styling, Insert.*

I. INTRODUCTION

It is trusted that the power utilization will increment 30% in forthcoming 25 years [1]. Those frameworks, that gives us power were grown long time previously and ordinarily utilize out of date foundation. Because of increments in day today utilization of power, load sheds has turned into a typical issue. There have been numerous cases recorded till now that has caused the enormous misfortune. as indicated by certain information records billions of dollars could be squandered in the power outage in us for instance, as of late there was a power outage in brazil in 2009, it went on for 4 hours and almost 50% of populace was influenced. so as to keep from these kinds of power outages, increasingly secure and dependable grid is required that gives and productive bidirectional correspondence among clients and the service providers [2] [3].

The idea of smart grid gives the promising outcome regarding giving productive and solid supply of power. the smart grid is productive when contrasted with existing matrix as a result of the utilization of certain new framework that was not presented previously. Generally sensors, smart meters, controls relays, phasor measurement units were presented that give better two way energy flow. Normally clients can apply their own optimal algorithms to buy least expensive power additionally they can build up their own power and can pitch it to smart grid. Likewise the utilization of smart grids enables the vitality providers to know about the requests identified with power continuously, so they can give ongoing help to their clients. In spite of the fact that this idea expanded the execution of smart grid at extremely high rate, yet it additionally influences the power distribution mechanism from multiple points of view. One of the significant dangers to brilliant networks is cyber attacks, due the presentation of a few new complex gadgets at different destinations, it worked out that these gadgets may go about as loopholes and can be utilized for infusing malware and exasperating the ordinary capacity of smart grid [4]. Likewise the presentation of internet like communication network adds fuel to flame by enabling intruders to get entrance from remote areas. Other than this there is likewise digital risk like malware, spyware, computer viruses that can cause such power unsettling influences.

In order to handle these circumstances different intrusion identification framework were created. These intrusion detection system were created improve the security of smart grid as far as both digital and physical attacks. in our exploration we will investigate the structure of the smart grid and furthermore examine different machine learning techniques that can decide if attack is happening or not. These machine learning techniques are utilized in this intrusion detection as structure models for investigating the power system aggravations.

A. Smart Grid Architecture

As we realize that there is a substantial communication network in the event of smart grid, thus so as to comprehend that systems we propose a three layer design of smart grid made out of Home Area Network(HAN), Neighboured Area Networks and Wide Area Network(WAN). Figure 1, shows the three layer architecture of smart grid.

Layer 1, HAN comprises OF Metering Module (MM) and Service Module (SM), and interruption recognition foundation for HAN. For deciding the ongoing utilization of information and cost for vitality to the end clients SM module is utilized while MM is utilized to record the utilization of the vitality in consumers. The interruption recognition module utilized in Home area networks tracks and checks both approaching and active communication [6].

Layer 2 comprises of neighbourhood area network. Its fundamental capacity is to gather metering and administration data from Home Area Networks. This layer is contained focal access controller and smart meter data gatherer. Focal access controller (FAC) goes about as halfway between the Host area network and vitality providers while as shrewd meter information gatherer (SMIG) stores the records of entire network as created by neighbouring HAN. Likewise this, every one of the information that moves all through NAN will be gone through NAN interruption identification module to recognize the malware.

The last and final layer is wide area network layer. This is an important layer and is generally in charge of giving broadband communication between the NAN, grid administrations, and substations and so on. Typically this layer has its own modules, for example, SCADA controller, energy distribution system EDS, and its very own intrusion detection module. IDS are required between SCADA controller and provider for security purposes.

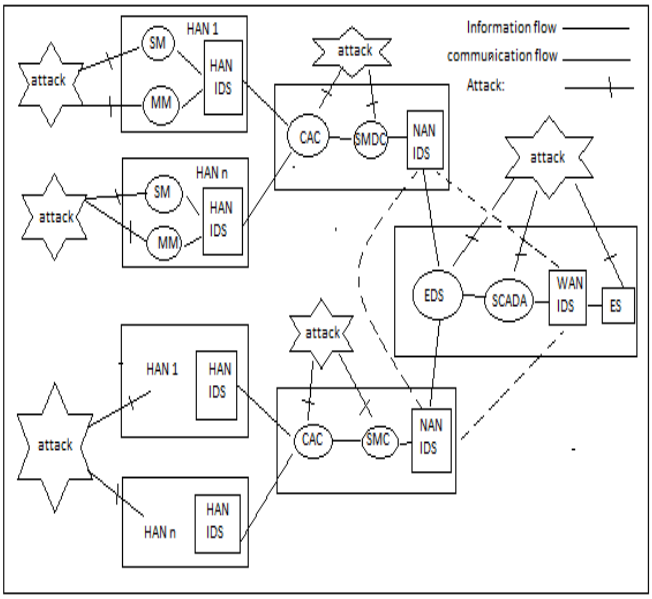

Fig 1:- Three Layer Architecture

Usually the communication topology that we have chosen for this type of architecture is the wireless mesh network. Mesh topology is used because of its several advantages. It provides multiple communication paths that prevents from the loss caused due to the natural failures as well as it is dynamic, self healing and scalable properties [8]. It also compensates the loss that can occur due to the malware injected in particular communication line.

B. Cyber Security Issues in Smart Grid

Despite the fact that the utilization of remote communication technologies builds the proficiency of smart grids, yet these advancements present the danger of new vulnerabilities and security related issues in the SMART GRID. As they become the flimsier focuses for the intruders to infuse the malware and thus prompts power system aggravations. Security of smart grid has turned into a vital issue. The privacy of the client's information is undermined because of increment in entry points and furthermore due presentation of malware. Some of the common issues faced by smart grid in terms of security are: Advanced metering security, Privacy of clients, Protocols utilized at various areas. So as to handle security related circumstances, it is important to build up a digital security system to ensure uprightness, accessibility and secrecy of the information transmission in savvy network. Interruption identification frameworks were worked for a similar reason [9] [10]. They are consolidated at each layer WAN, NAN, HAN layers and gives a procedure to distinguishing the security dangers or malware that influence the correct capacity the smart grid.

II. PROPOSED SOLUTION

A direct arrangement is to create specific intrusion detection model that can precisely distinguish all the security attacks. Typically, Machine learning has been utilized as a discriminator between anomalous events in intrusion detection for digital security systems. In this work, we will investigate the utilization of ML in discriminating power system disturbances. Normally digital attacks have same impact as that of natural events. So it is incomprehensible for human to separate between the common and vindictive occasions thus ML strategies utilize a few arrangement calculations to recognize these assaults.

C. Machine Learning Approach

Machine learning is a particular discipline that involves the programming of a machine in such way that it automatically learns and improves with experience. The difference between traditional programming and Machine learning is that, in case of traditional programming we know the Input and rules and the output is generated. But, in case of Machine learning approach output and input is already known and we have to generate certain rules. In machine learning the training of machine takes place by feeding data, it allows machine to automatically learn without any programming involved. By using machine learning algorithms, the attack events and the natural events can be easily classified and hence can easily distinguish whether any power system disturbance have occurred or not. In case of Machine learning, supervised machine learning techniques are generally used for classification purposes. Supervised learning algorithms take learning samples and return a function or model. Usually, learning samples are the combination of input and output pairs. Attribute values can be continuous or discrete. At any time if the output takes its qualities in a discrete set, then this is a classification problem and when it's continuous then this is a regression problem. The fundamental property of classification algorithms used is the ability of these algorithms to make the predictions.

The combination of Home area network and the classification algorithm models centres around better grouping of malicious attacks by preparing vast measure of information that has been gathered from various hardware

equipment introduced in smart grid. If attacks can't be characterized by home network layer then data is sent to the higher layers such WAN and NAN for further assessment. These layers have their own Intrusion recognition modules and use separate classification models.

D. Some Machine Learning Techniques

Intrusion detection system makes use of several computational intelligence algorithms for detecting the vulnerabilities at faster rate**.** Some of the popular algorism that is used in Intrusion detection module is given below:

➢ *Clonal Selection Classification Algorithm*

This calculation can be clarified in comparative style as how a solitary B or T cell that recognizes an antigen entering in our body is chosen from a pool of effectively existing cells with various antigens and afterward repeat to frame a clonal cell populace to totally dispose of the antigens [11]. This property of immune system and its nature can be acknowledged and connected in network intrusions detection also. In light of the idea of clonal calculation Artificial insusceptible recognition system (AIRS} is created. It is an immune based supervised learning calculation which comprises of clonal segments, affinity acknowledgment balls and so forth. Typically it is cluster based methodology utilized for grouping of information arranged by improving cluster centres.

➢ *Support Vector Machine*

SVM is the most powerful tool that can be used for the classification of the data. SVM usually classifies data by applying the two different principles: Large margin separation and Kernel function [12]. Large Margin separation usually is technique in which the separation line generated in such a manner that the distance between the line and the margin (closest point to the line) is maximised. Usually these types of separation can only occur when data is sparse in single dimension and hence data is linearly separable. In case nonlinear classification Kernel functions are used that similarity between two data points. In kernel function , generally hyper planes are used to separate data instead of lines. In order to draw an hyper plane, the mapping of data to different space is done so that hyper plane could easily classify the data.

In case of non linear and non separable data a complex quadratic equation needs to be solved in order to generate hyper plane, the equation is of the form Min

$$\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{l}\xi_i$$

$$y_i(w^T\phi(x_i)+b) \geq 1-\xi_i$$

$$\xi_i \geq 0$$

Where w is weight vector, C is controls variance between margin maximization and error minimization. ϵ_I is a set of a slack variable, y_i denotes the unique constraint, b is bias, xi is the training vector, and $\varphi(x_i)$ denotes the kernel function.

➢ *Artificial Nueral Network*

This type of technique is most advanced and most reliable techniques that can be used for both supervised as well as unsupervised learning. In case of supervised learning radial function neural networks are used to detect the attack events because of their quick learning ability. In this type of algorithm, neural network model has three layers and in order to train the data, two stage learning process of data takes place. Usually, the parameter (Weight and Bias) in the hidden layers are adjusted in such a way that minimum loss is obtained at the output and hence model could accurately predict the outcome. Grid based approach is followed for data clustering and compression. Also various optimising functions such as sigmoid, RELU, Softmax etc are used to amplify or decrease the results of output.

III. PERFORMANCE EVALUATION

Confusion matrix shown in table 1 is by far one of the best tools to evaluate the performance of the models employed. The output yielded by a confusion matrix is used to calculate the accuracy along with certain other parameters required to determine the performance metric. These outcomes act as the indicators in order to check the Classifier Performance. Usually four outcomes are generated due to binary classifications, which are as:

- True positive (TP) which is the correct positive prediction.
- False Positive (FP) which is the incorrect positive prediction.
- True negative (TN) which is the correct negative prediction.
- False negative (FN) which is the incorrect negative prediction.

		Predicted	
		Positive	***Negative***
Observed	***Positive***	TP	FN
	Negative	FP	TN

Table 1

Though accuracy is the overall measure of performance, there are some other measures that can provide us the better vision of how accurately the classifier works. These are precision, recall, F1 score etc. These measures are calculated through the values obtained from confusion matrix.

IV. CONCLUSION

In this paper, we have explored the smart grid qualities as compared to that of an ordinary grid. We have also seen that smart grid is prone to security attacks. These intrusions can be carried out from remote location and are dynamic in nature. We have proposed the concept of Intrusion detection system that can be introduced at different layers of smart grid and uses certain machine learning models to classify attack and natural events. We centred our approach on supervised learning and artificial neural networks .These approaches are helpful in classifying these events and detection of root cause behind power disturbances, hence increasing the performance of smart grid.

REFERENCES

[1] Safaric, S. & Malaric, K. (2006). "ZigBee wireless standard" 48th International Symposium ELMAR-2006, Zadar, Croatia, 07—09. (p.259-262).
[2] Lee, M. J. & al., (2006). Emerging Standards for Wireless Mesh Technology. IEEE Wireless Communication.
[3] Garcia-Hernandez, C. F., Ibarguengoytia-Gonzalez, P. H., & Perez-Diaz, J. A. (2007). Wireless Sensor Networks and Applications: A Survey. IJCSNS International Journal of Computer Science and Network Security, 7(3). (p.264-273).
[4] Freund, Yoav, and Robert E. Schapire. "A decision-theoretic generalization of on-line learning and an application to boosting." Journal of computer and system sciences 55.1, 119-139. 1997.
[5] McLaughlin, K.; Sezer, S.; Littler, T.; Pranggono, B.; Brogan, P.; Wang, H.F., "Intrusion Detection System for network security in synchrophasor systems," IET International Conf. , vol., no., pp.246,252, 27-29, April, 2013.
[6] B. Martin, "Instance-based Learning: Nearest Neighbor With Generalization" University Of Waikato, 1995.
[7] M. Talebi, J. Wang, Z. Qu, "Secure Power Systems Against Malicious Cyber-Physical Data Attacks: Protection and Identification," World Academy of Science, Engineering and Technology, vol. 66, 2012.
[8] Berthier, R., Sanders, W., & Khurana, H. (2010). Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions. In First IEEE International Conference on Smart Grid Communications (SmartGridComm). (p. 350–355).
[9] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. IEEE International Conference on Computational Intelligence for Security and defense applications. (p. 53-58).
[10] Hooper, E. (2010). Strategic and Intelligent Smart Grid Systems Engineering. Internet Technology and Secured Transactions (ICITST), 2010 International Conference, London, 8-11. (p.1-6).
[11] R. Perdisci, G. Gu, and W. Lee., "Using an Ensemble of One-class SVM Classifiers to Harden Payload-based Anomaly Detection Systems", Proc. International Conf. on Data Mining, pages 488–498, 2006.
[12] R.C. Holte, "Very Simple Classification Rules Perform Well On Most Commonly Used Datasets," Machine Learning, Vol. 11, No. 1, Pp. 6390, 1993.