FPGA Based Distributed Network Intrusion Detection in Wimax Environment of Smart Grids Using SVM

N. Purnima[1]
PG Student (Communication Systems)[1]
Velammal College of Engineering and Technology,
Madurai-625009

Omprakash P[2]
Assistant Professor[2]
Velammal College of Engineering and Technology,
Madurai-625009

Abstract

The next generation electric grid will depend on a complex network of computers, software, and communication technologies. It also has to face many cyber security threats because of the complex networks in the entire system like IEEE 802.15.4, IEEE 802.11, and IEEE 802.16 Standards. Each of these will expose the power grid to cyber security threats. In order to address this issue, this work proposes distributed intrusion detection for smart grids (SGDIDS), in multiple layers of the smart grids. Advanced Metering Infrastructure (AMI) is the consumer devices in home which also faced by cyber security threats. This paper proposes the intrusion detection mechanism to detect the cyber security threats in smart grids using Support Vector Machine (SVM).

1. Introduction

The smart grid promises the world an efficient and intelligent approach of managing energy supply and consumption. It has advantage of the convenience, reliability, and energy savings provided through real time energy management. One of the advantages of the smart grid is two-way communication network between energy suppliers and their customers. This allows the smart grid to be viewed as a electric grid that has an integrated data communication network allowing the collection and analysis of data at all levels in real time. This communication network will provide a number of new energy concepts including real-time pricing, load shedding, consumption management, cost savings from peak load reduction and energy efficiency, integration of plug-in hybrid electric vehicles for grid energy storage, and the integration of alternative distributed generation sources including photovoltaic systems and wind turbines. This new communication network will be constructed using various communication paths including fibre optic cable, twisted pair, and broadband over power line, and wireless technologies. In this paper we propose a new technology of Wimax in Smart Grid communication network. The proliferation of this new technology, especially an Internet-like communications network, may introduce some new threats to the security of the smart grid. Security has to be given to advance metering Infrastructures or Smart Meters.

2. Wimax

Wimax is the first commercially available 4G technology. It is ideally suited to meeting both the requirements of smart grid applications and the needs of utilities to keep complexity under control without sacrificing security or reliability. Utilities have long operated proprietary networks, and know well that they often carry a hefty price tag, limit their ability to innovate and upgrade, and keep them tied to a vendor. Wimax is not a technology specifically developed for utilities. It has wide appeal among network operators that provide services within public. Wimax also has support from many infrastructure and terminal device vendors because of its long coverage area.

2.1. Role of Wimax within Smart Grids

The role of Wimax within different smart grid implementations will vary depending on the utility's requirements and existing infrastructure, the availability of wireline connectivity, and the overall environment in which the utility operates. Wimax is a versatile technology that can be deployed in multiple roles.

2.1.1 Backhaul. Wimax can provide the backhaul link to the network operating centre (NOC) Wimax can transport application data from and to terminal devices. This is likely to be the case for many smart meter applications, at least initially, with meters transmitting data to concentrators that in turn are connected with Wimax base stations.

2.1.2 Last-mile connectivity. Wimax can also be directly connected to terminal devices. Wimax will become widely used as a module to connect smart meters directly to the Wimax network. Smart meters with Wimax modules are more likely to be employed in rural, low-density areas, where Wimax base stations can cover wide areas and may result in cost savings over the concentrator model.

2.1.3. Mobility. A Wimax network can also provide connectivity to the mobile workforce and to service vehicles, using the same network infrastructure that supports connectivity to fixed terminals and backhaul.

2.1.4. Emergency. Mobile base stations and terminal devices can be moved to emergency areas to create temporary networks, which may use Wimax, satellite, or other technologies for backhaul. In this case, the same devices used by the mobile workforce and in service vehicles and fixed locations can be used to connect to the temporary base station. Intrusion detection system (IDS) is necessary for protecting SMART GRIDS. Intrusion detection is the process of monitoring the threats occurring in a computer system or network. The performance of IDS is evaluated based on three main measures including:

False positive (FP): An event signalling an IDS to produce an alarm when there is no attack taken place. The formula by which FP is calculated is:

$$\mathrm{FP} = \frac{\text{Number of normal patterns detected as attack}}{\text{Number of all normal patterns in the network}}$$

False negative (FN): A failure of the IDS to detect an actual attack. FN is calculated using below formula:

$$\mathrm{FN} = \frac{\text{Number of attacks not detected by IDS}}{\text{Number of attacks in the netork}}$$

Detection Rate: The ability of IDS to detect all the existing attacks and is calculated by

$$\mathrm{DR} = \frac{\text{Number of detected attacks}}{\text{Total number of attacks targeting the network}}$$

IDS are an extendable solution and it can be deployed in communication network of Smart Grids with various sizes. In addition, we can extend the IDS in a way that it can detect more number of attacks by placing more IDS in the network and equipping IDS with corresponding detection techniques**.**

Table 1. Lists of attacks targeting different OSI layers

ATTACK	LAYER
Physical Layer	Signal Jamming
Mac Layer	Link Layer jamming, MAC spoofing
Network Layer	Rushing, Wormhole, Black hole, Packet dropping
Transport Layer	SYN flooding, Data injection

3. SVM Classifier

Machine learning via SVM is a powerful tool for the classification of data [5]. SVM is a type of machine learning technique that attempts to successfully classify sets of data by leveraging two basic principles: large-margin separation and kernel functions. Large-margin separation refers to the idea that when classifying data it is sensible to draw a line of separation in such a manner that the distance between that line and the closest data point on either side of that line is maximized. Kernel functions are algorithms or functions that calculate the similarity between two points and must be used if nonlinear classification boundaries are required. Generally speaking, as the dimension of classification increases hyper planes are used to separate the data instead of lines. This is completed by mapping the data to a different space (also using a kernel function) where a hyper plane is able to classify the data. In order to achieve a classification based on these ideas, a convex, quadratic program must be solved that is, in the case of data that is nonseparable, of the form

$$\min \frac{1}{2} \ \|\omega\|^2 + \mathrm{C}\sum_{\mathrm{i}=1}^{\mathrm{l}} \varepsilon_{\mathrm{i}} \qquad (1)$$

$$\mathrm{y_i}(\omega^{\mathrm{T}}\varphi(\mathrm{x_i}) + \mathrm{b}) \geq 1 - \varepsilon_{\mathrm{i}} \qquad (2)$$

$$\varepsilon_{\mathrm{i}} \geq 0 \qquad (3)$$

where is the weight vector, C is a value that and controls the variance between margin maximization and error minimization, ε_i is a set of slack variables that measure constraint violation, $y_i$denotes that there is a unique constraint for each necessary classification i,b is the bias, $x_i$is a training vector, and $\varphi(x_i)$ is the kernel function that maps the training or testing vector to a different space [6], [7]. The formulation is the equivalent of maximizing the margin while also minimizing error.

Often it is also necessary to classify data into three or more categories. Two methods are typically used to perform this classification: the one-against-many and the one-against-one approach.

The former approach is simpler and examines one category at a time while merging the remaining categories into a single category. This allows for simple, binary classification. The latter approach is more computationally intensive though more accurate as it creates $\frac{k(k-1)}{2}$models in order to classify all data where k is the number of classifications required.

4. VHDL Based Network Intrusion Detection

Smart Grid Communication Network IEEE 802.16 standard in which Smart Grid Network Intrusion Detection System is modelled and implemented using the VHDL Very high speed integrated circuit- Hardware Description Language. Evaluation of the SGDIDS (Smart Grid Network Intrusion Detection System) is done through simulation. Simulation is done for the testing dataset of Support Vector Machine Classifier. In our paper for example we took the protocols such as Transmission Control Protocol and IPv4 in which packet normalization is done first to train the dataset using Support Vector Machine Classifier.

5. Software Used

This paper uses the software Questasim VHDL simulator produced by Model Technology. This is a powerful commercial simulator that can handle both the VHDL and Verilog hardware description languages. These results are obtained using "questasim_6.4c" downloaded from Mentor graphics.

6. Packet Normalization

Pkt_norm (Packet Normalization) can be shredded in transit, and processing these shards of data can increase system load. The system at one end of the connection might have a habit of braking up transmitted packets into tiny bits or perhaps some router in the middle thinks that our packets are too large and splits them up to digest them more easily. So, instead of nice whole packets our network will receive small bits or fragments.

Packet normalization is done here for the TCP and IPV4 protocols. The UDP and IPV4 can also be done depends upon the packets. In the Packet Normalization the TCP and IPv4 data fed in the backend program. The packet arrives later will be compared with the Support Vector Machine training dataset. If the incoming packet does not match the packets of the trained dataset, then they will display as attacked packets. If the incoming packet matches the packets of the trained dataset, then they will display as normal packets. Output waveform for the packet normalization coding is obtained in Questasim software of VHDL and which is represented in below figure 1.

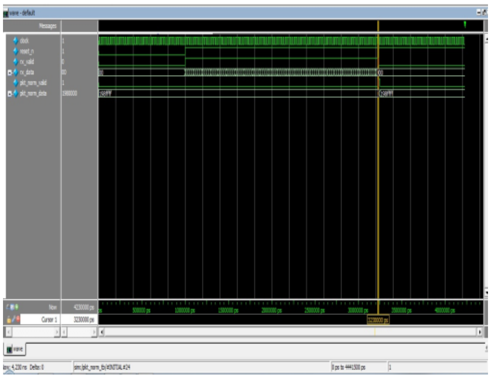

Figure 1. Representation of packet normalization

7. Training Data

Support Vector Machine training set we are fixing the values according to the substation of the Smart Grids. The values of the data differ for each substation. After finding the values for each substation we are given those values as the training data set to the training algorithm of the Support Vector Machine Classifier. The incoming packets may belong to any type of class i.e. it may be a attacked packet or may be a normal incoming packets. Form the training dataset the Bayes classifier will test the incoming packets. Output waveform obtained in the questasim_6.4c for the training data is represented in the below Figure 2 to find the attacked packets in Smart Grids.

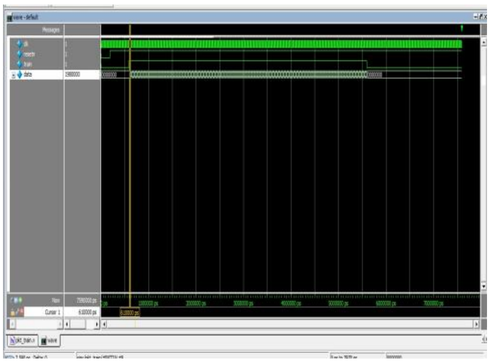

Figure 2. Representation of training data using support vector machine classifier

8. Normal Packets

The output waveform obtained in the Questasim for the normal packets is represented in the Figure 3. Once the testing starts, the testing dataset will compare the packets with the trained dataset. If the incoming packet matches the packets of the trained dataset of the Support Vector Machine Algorithm, then output will display as normal packets.

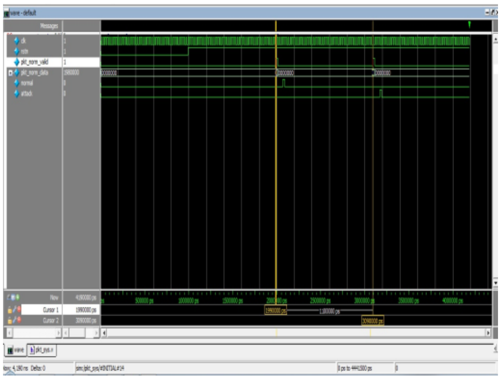

Figure 3. Representations of normal packets

8. Attacked Packets

These are the waveform for the attacked packets. Once the testing starts, the testing dataset will compare the packets with the trained dataset. If the incoming packet does not match the packets of the trained dataset of the Support Vector Machine Algorithm, then output will display as attacked packets. Output waveform for the attacked packets is obtained in Questasim software of VHDL and which is represented in below figure 6.4.

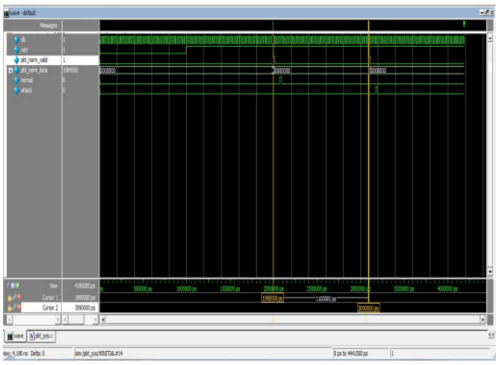

Figure 4. Representation of attacked packets

9. Conclusion

In this paper the Quality of Service is increased, security and faster transmission of data is also increased in Smart Grid's Wimax based communication network. The Wimax environments are secured from many threats, since SGDIDS found the attacks using Support Vector Machine Classifier. The percentage of the attacked packets is found by classification of the data according to the Support Vector Machine which differ for each substation in the Smart Grids. Hardware behaviour will directly reflect because of using VHDL based Smart Grids Network intrusion Detection (SGDIDS). The FPGA based intrusion detection produces faster and accurate method for finding the attacked packets in the Wimax communication network of Smart Grid.

10. Reference

[1] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Appl. Soft Comput.*, vol. 10, no. 1, pp. 1–35, 2010.

[2] [Mentor] Mentor Graphics Company

[3] Ruiz-Llata, G. Guarnizo, and M. Y?benes-Calvino. FPGA implementation of a support vector machine for classification and regression. *WCCI 2010 IEEE World Congress on Computational Intelligence, IJCNN*, july 2010

[4] [IEC61850] International Electrotechnical Comission (IEC) 61850.J. Cho, B. Benson, S. Cheamanukul, and R. Kastner. Increased performance of FPGA-based color classification system. *Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, pages 29–32, 2010.M.

[5] D. Kim and J. Park, "Network based intrusion detection with support vector machines," in *Proc. ICOIN*, 2003, vol. 2662, Lecture Notes in Computer Science, pp. 747–756.

[6] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*,vol. 20, pp. 273–297, 1995[Online].Available:http://www.springerlink.com/index/K238JX04HM87J80G.pdf

[7] S. R. Gunn, "Support vector machines for classification and regression,"Faculty Eng., Sci., Math. School Electron. Comput. Sci., Tech.Rep., May1998[Online].Available:http://pubs.rsc.org/en/Content/ArticlePDF/2010/AN/B918972F/2009-12-23