International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 6 Issue 6 November 2016
International Manuscript ID : 2249054XV6I6112016-12

DETECTION AND PREDICTIVE ANALYSIS OF ATTACKS IN TRANSPARENT OPTICAL NETWORKS

Priyanka
Assistant Professor, EE Department
YMCA University of Science and Technology
Faridabad, Haryana, India

ABSTRACT

Traditional transport networks are made of optical fiber-based links between telecommunications offices, where multiple wavelengths are multiplexed to increase the capacity of the fiber. The wavelengths are terminated on electronic devices called transponders, undergoing an optical-to-electrical conversion for signal Re-amplification, Reshaping, and Retiming (3R). Inside a telecommunications office, the signals are then handled to and switched by a transport switch (aka optical cross-connect or optical switch) and either are dropped at that office, or directed to an outgoing fiber link where they are again carried as wavelengths multiplexed into that fiber link towards the next telecommunications office. The act of going through Optical-Electrical-Optical (O-E-O) conversion through a telecommunications office causes the network to be considered opaque. When the incoming wavelengths do not undergo an optical-to-electrical conversion and are switched through a telecommunications office in the optical domain using all-optical switches (also called photonic cross-connect, optical add-drop multiplexer, or Reconfigurable Optical Add-Drop Multiplexer (ROADM) systems), the network is considered to be transparent. Hybrid schemes that leverage optical bypasses and provide limited O-E-O conversions at key locations across the network, are referred to as translucent networks. ROADM-based transparent optical mesh networks have been deployed in metropolitan and regional networks since the mid-2000s. In the early 2010s, operational long distance networks still tend to remain opaque, as there are transmission limitations and impairments that prevent the extension of transparency beyond a certain point. This manuscript present the security and related performance aspects in the transparent optical networks with assorted dimensions.

Keywords - ANN, Induction Motor, Optical Communications

INTRODUCTION

A wavelength-routed optical network consists of multi-wavelength cross-connect switches (XCSs) which are interconnected by optical fibers [1].

Some (or all) cross-connects, referred to as nodes in this paper, are also attached to access stations where data from several end-users could be multiplexed onto a single wavelength division multiplexed (WDM) channel[2. An access station provides optical-to-electronic (O/E) conversion and vice wersa to interface the optical network with conventional electronic equipment. The access station, at an intermediate node, may also be used (as in this study) for signal regeneration on a lightpath. A new call is admitted into the network if a light-path (a set of free wavelengths along a given route from source to destination) can be established between the call's source and destination stations. Depending on the number of all-optical fragments in a single lightpath, three different approaches may be employed to operate such a network.

These approaches are: transparency, opacity, and translucency. Transparency, in the strict sense, implies that the physical medium should support end-to-end communication of data, independent of bit rates and signal formats. Transparent WDM networks readily allow express signals to bypass extensive electronic signal processing at intermediate nodes. However, the quality of an optical signal degrades as it travels though several optical components along its light-path from its source to destination [3]. The causes of these degradations include optical-fiber nonlinearities; chromatic and polarization-mode dispersion; noise accumulated due to amplified stimulated emission (ASE) from optical fiber amplifiers (e.g. erbium-doped fiber amplifiers (EDFA)); effects of non-flat gain profile and gain saturation in fiber amplifiers; cross-talk introduced at cross connects; etc. To overcome these impairments, "long-distance" lightpaths may require signal regeneration, at one or more intermediate locations in the network, to "clean up" the signals. Signals are regenerated either through an opto-electronic conversion followed by an electro-optic conversion (as assumed in this study) or entirely in the optical domain. At the other extreme of the spectrum from fully transparent networks are fully opaque networks, which include such signal regenerators at every intermediate node along a lightpath. Hence, in opaque networks, a single optical hop of a light-path never spans more than one physical fiber link in the network.

PROPOSED WORK

In proposed work, a unique model shall be developed and training will be done using ANN with fuzzy mathematical model so that the penetration level and prediction of malware can be done. To facilitate the detection of unknown malware based on the generalization of the behaviour of known malwares, we propose training supervised ANNs using known malwares.

Artificial neural networks are extracted from biological neural networks and then introduced in solving many real world problems [4]. Artificial neural network based intelligent model will be trained to recognize the characteristics of malicious code by looking at various examples of malware and non-malware files, could perhaps offer a far better way to catch such nefarious code. An approach known as deep learning, which involves training a network with many layers of simulated neurons using huge quantities of data, will be tested in the proposed work. Basically a neural network comprises of two or more layers. The layers are input layer, hidden layer and output layer. As the number of hidden layers increases the accuracy of the results also increases

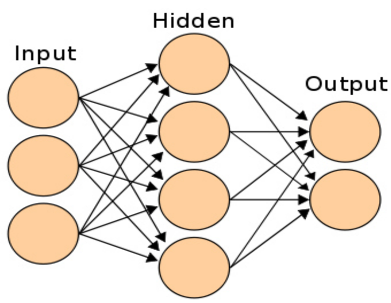

Figure 1- The Layers of ANN

A neural network works on two types of learning algorithms, supervised learning algorithm and unsupervised learning algorithm.For these reasons, we propose employing ANN models for the detection of malwares.

Artificial Neural Networks (ANN) refers to the high level metaheuristic approach to achieve the excellent efficiency in training the datasets in multiple domains.

The major advantage of neural networks is that it learns through the training data, then updates its weights and gives an accurate result thus giving the high level of efficiency in real-time operations, low consumption of CPU resources during the classification phase, and its ability to generalize, which is important for detecting any previously unseen malwares.

Figure is the classical format and diagrammatic structure of ANN. In the figure there are number of components which work together for the generation and prediction of the datasets.

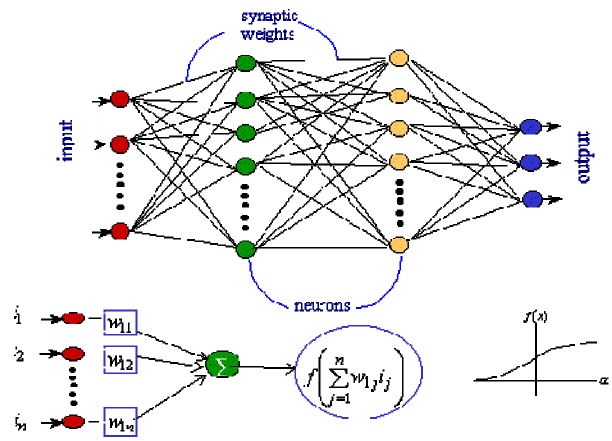

Figure 2 – Classical Architecture of Artificial Neural Network [36].

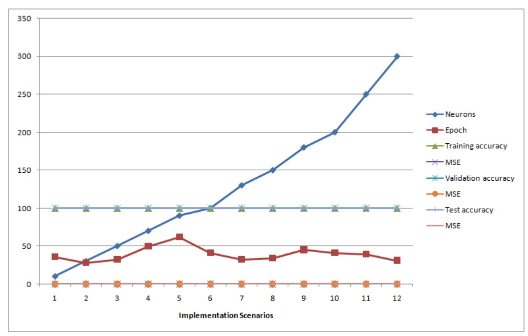

Figure 3 – Cumulative Analysis of parameters in implementation

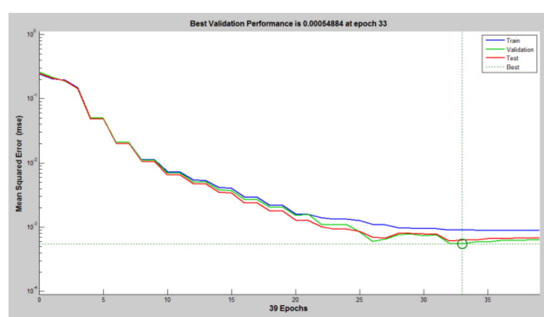

Figure 4 – Performance Plot of the Optimal and Higher Efficiency ANN Model

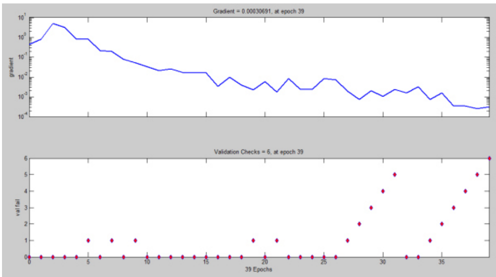

Figure 5 – View Validation Checks and Gradient for optimal set of neurons and layers

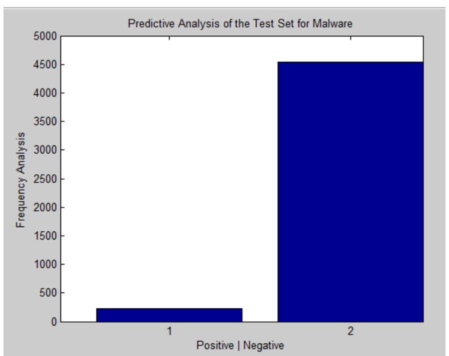

Figure 6 – Predicted Positive and Negative Probabilities for Sample dataset

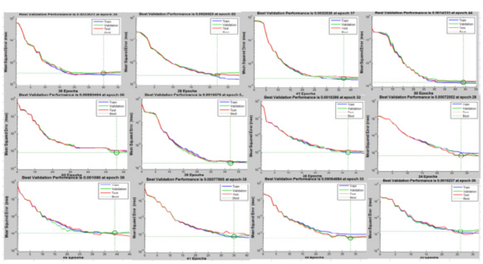

Figure 7 – Performance Plots for assorted implementation scenarios

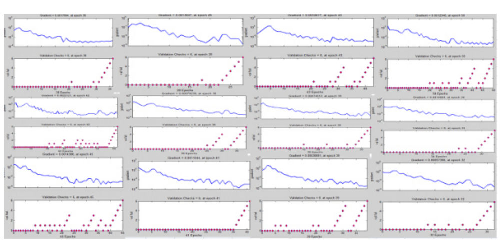

Figure 8 – Gradient and Validation Plots for assorted implementation scenarios

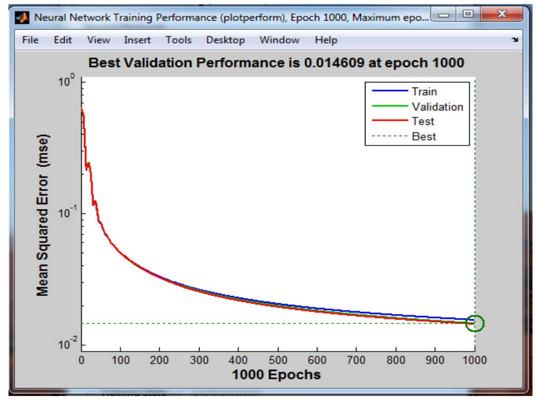

Figure 9 – View of Performance Plot under scenario

The mean squared error in the above figure obtained after simulation is as per the expectations. The error factor is reducing and towards the zero level determining that the eventual and progressive epochs are giving effective results with very less error rate. At the initial level, the error factor is more which should be towards downline and zero error line.

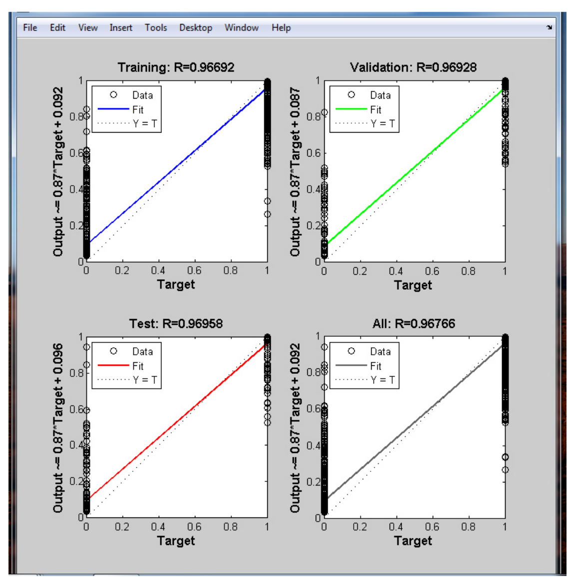

Figure 10 - Validation Plots and Assorted Views

Figure 11 – Generation of confusion matrix under scenario

CONCLUSION AND FUTURE WORK

This work is giving effective results in terms of very less error rate and high efficiency in getting the probability factor of malware still this work can be further enhanced using other optimization approaches. In this work, the metaheuristic approach for optimization is done. There exist another approach hyper-heuristic that can be integrated for deep learning of malware and predictive analysis. The fundamental difference between metaheuristics and hyper-heuristics is that most implementations of metaheuristics search within a search space of problem solutions, whereas hyper-heuristics always search within a search space of heuristics. Thus, when using hyper-heuristics, we are attempting to find the right method or sequence of heuristics in a given situation rather than trying to solve a problem directly. Moreover, we are searching for a generally applicable methodology rather than solving a single problem instance.

Hyper-heuristics could be regarded as "off-the-peg" methods as opposed to "made-to-measure" metaheuristics. They aim to be generic methods, which should produce solutions of acceptable quality, based on a set of easy-to-implement low-level heuristics. In terms of enhancement and further optimization, the swarm intelligence approaches can be used which includes nature inspired algorithms. Swarm intelligence is the discipline that deals with natural and artificial systems composed of many individuals that coordinate using decentralized control and self-organization. In particular, the discipline focuses on the collective behaviors that result from the local interactions of the individuals with each other and with their environment. Examples of systems studied by swarm intelligence are colonies of ants and termites, schools of fish, flocks of birds, herds of land animals. Some human artifacts also fall into the domain of swarm intelligence, notably some multi-robot systems, and also certain computer programs that are written to tackle optimization and data analysis problems.

REFERENCES

[1] Bindhaiq, S., Supa, A. S. M., Zulkifli, N., Mohammad, A. B., Shaddad, R. Q., Elmagzoub, M. A., & Faisal, A. (2015). Recent development on time and wavelength-division multiplexed passive optical network (TWDM-PON) for next-generation passive optical network stage 2 (NG-PON2). Optical Switching and Networking, 15, 53-66.

[2] Lei, T., Zhang, M., Li, Y., Jia, P., Liu, G. N., Xu, X., ... & Niu, H. (2015). Massive individual orbital angular momentum channels for multiplexing enabled by Dammann gratings. Light: Science & Applications, 4(3), e257.

[3] Shoaie, M. A., Vedadi, A., & Brès, C. S. (2015, September). A simple all-optical format transparent time and wavelength demultiplexing technique for WDM & Orthogonal-TDM Nyquist channels. In Optical Communication (ECOC), 2015 European Conference on (pp. 1-3). IEEE.

[4] Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, 61, 85-117.

[5] Chandwani, V., Agrawal, V., & Nagar, R. (2015). Modeling slump of ready mix concrete using genetic algorithms assisted training of artificial neural networks. Expert Systems with Applications, 42(2), 885-893.

[6] Macedo, M. N. Q., Galo, J. J. M., De Almeida, L. A. L., & Lima, A. D. C. (2015). Demand side management using artificial neural networks in a smart grid environment. Renewable and Sustainable Energy Reviews, 41, 128-133.