ISSN: 2250–3676

[IJESAT] INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & ADVANCED TECHNOLOGY Volume-2, Issue-3, 396 – 400

SECURITY IN AON USING ARTIFICIAL NEURAL NETWORK

Inadyuti Dutt[1], Soumya Paul[2], Rahul Das[3]

[1]*Asst. Professor, Dept. of Computer Application, B.P.Poddar Institute of Management & Technology, West Bengal, India,* ***inadyuti@gmail.com***

[2]*Assoc.Professor & Head, Dept of Computer Application, B.P Poddar Institute of Management & Technology, West Bengal, India,* ***soumya.paul2000@gmail.com***

[3]*Software Programmer, Cognizant Technology Solutions, West Bengal, India,* ***rahulzmailbox@yahoo.in***

Abstract

The security in an All-Optical-Network (AON) becomes a major concern when huge user data related to sensitive information have to be transported along a channel. The paper attempts to unfold attacks on the channels with the help of the concept called Artificial Neural Network (ANN). A neural network consists of an interconnected group of neurons, and it processes information using a connectionist approach to computation. This paper proposes two algorithms for attack detection and management in AON. The first algorithm detects attack using the concepts of ANN, where the input function is computed with the help of synaptic weights given to each such input. The resultant input function is used to determine whether an attack has really occurred on an optical node in a network or not. Based on some pre-assumed value of input function to be the idealistic value the computed value of input function is compared to detect whether an attack has been encountered by the node or not. The second algorithm works once the attack has been detected on an optical node. The node which computes the attack in its first hand propagates the attack/alarm message to the Controller. The Controller conveys the attack message to all other neighbouring nodes which can be affected by the attacked node.

Index Terms*: All-Optical-Network (AON), Artificial Neural Network (ANN)*

----------***----------

1. INTRODUCTION

The next generation wavelength division multiplex (WDM) optical network transports a huge user data and contains sensitive information, personal information like bank account number, credit card number. And for this reason, there are two important consequences:

* A good part of the huge aggregate traffic is sensitive and confidential, and it will be attractive to malicious attackers to eavesdrop, mimic the source or cause denial of service [1].

* Even short service interruptions due to failures and severe degradations [2-3] can cause network congestion and/or traffic loss.

As a result, there are two types of security in communications, user data securing and physical network securing. User data security can be addressed with encryption algorithms. Physical network security, and particularly the WDM fiber-optic network, has just begun to be addressed [4]. Current methods rely on optical power detection and on monitoring the bit error rate (BER) of a channel's performance, which however are neither conclusive nor very fast [5].

The next generation optical network is vulnerable to malicious attacks to eavesdrop, mimic the source or cause denial of service. In this paper we propose an algorithm that proactively detects an attack in an All-Optical Network and conveys the attack message to the all neighbouring optical nodes using the concepts of Artificial Neural Network.

1.1. Artificial Neural Network

An Artificial Neural Network (ANN), usually called Neural Network (NN), is a mathematical model or computational model that is inspired by the structure and/or functional aspects of biological neural networks. A neural network consists of an interconnected group of neurons, and it processes information using a connectionist approach to computation. In most cases an ANN is an adaptive system that changes its structure based on external or internal information that flows through the network during the learning phase. An artificial neural network consists of a pool of simple processing units which communicate by sending composed of units that perform similar tasks. First layer of a multilayer ANN consists of input units. These units are known as independent variables in statistical literature. Last layer contains output units. In statistical nomenclature, these units

are known as dependent or response variables. All other units in the model are called hidden units and constitute hidden layers. There are two functions governing the behaviour of a unit in a particular , which normally are the same for all units within the whole ANN, i.e. the input function, and the output/activation function. Input into a node is a weighted sum of outputs from nodes connected to it. Fig. 1 represents the mathematical representation of neural network. The input function is normally given by equation (1) as follows:

$Net_i = w_{ij}\, x_{ij} + \mu_i$

where Net_i describes the result of the net inputs weighted by the weights impacting on unit i. Also w_{ij} are weights connecting neuron j to neuron i. The x_{ij} is the output from unit j and is a threshold for neuron i. Threshold term $\mu_{i,}$ is baseline input to a node in absence of any other inputs. If a weight w is negative, it is termed inhibitory because it decreases net input, otherwise it is called excitatory.

Each unit takes its net input and applies an activation function to it. The output of a neuron is a function of the weighted sum of the inputs plus a bias. The function of the entire neural network is simply the computation of the outputs of all the neurons. It is entirely a deterministic calculation.

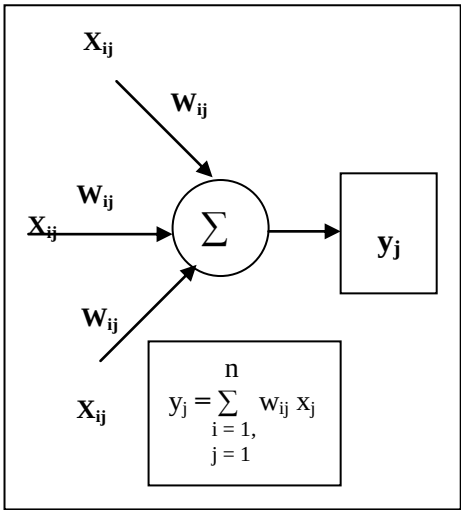

Fig-1: Mathematical representation of neural network

1.2. Proposed Approach using Artificial Neural Network

Artificial Neural Network is inspired from the biological neural system in human brain and body where numerous neurons cooperate to perform a desired function with inputs coming from synapses. The concept of neural system is used in ANN where the synapses correspond to inputs and neurons relate to the processing units. The signals coming from the neurons in neural system can be compared with the desired outputs from the processing units in ANN.

In general, ANN's approach attempts to solve a problem in a better way because of the two following factors:

i. Ability to learn

ANN figures out how to perform their function on their own. Determine their function based only upon sample inputs.

ii. Ability to generalize

It produces reasonable outputs for inputs it has not been taught how to deal with.

In AON, ANN technique can be utilized to get better and faster results in attack detection. In AON, the optical nodes are interconnected to each other using different topologies. Each node in AON takes a set of inputs for the input function from an external node or hacker and tries to match them correctly with the help of the output/activation function. If the inputs with the weights assigned using ANN compute to get correct output then there exists no active security attack. But after the computation if it produces incorrect output then an attack is said to be detected.

Though other approaches like Genetic Algorithm (GA) can also detect the attack but may incur a very large setup delay because they require a time consuming random searching process to generate the first population of cycles after the arrival of a new input.

1.3. Outline of remaining sections

The paper is organized as follows: Section 2 is the body of the paper, which states the problem statement based on ANN technique in subsections, 2.1 and 2.2. The detailed description of the proposed ANN based algorithm for attack detection and greedy algorithm for attack management are described in the Sections of 3 and 4 whereas Sections 5 shows the results and finally the paper concludes in Section 6.

2. PROBLEM STATEMENT

An artificial neural network based algorithm for attack detection has been designed. This work proposes an extension to the ANN framework. Network security in AON using Artificial Neural Network (ANN) uses this approach to detect any attack on a given optical node of an AON. Given an AON, say in a mesh network, has four optical nodes connected to each other as shown in Fig. 2. There exists a Controller which takes care of the attack detection and attack management. The proposed algorithm has to parts namely: Attack detection and Attack management. The Controller vigil constantly the network for attack detection and once it finds so conveys the attacked node message to all its neighbouring nodes.

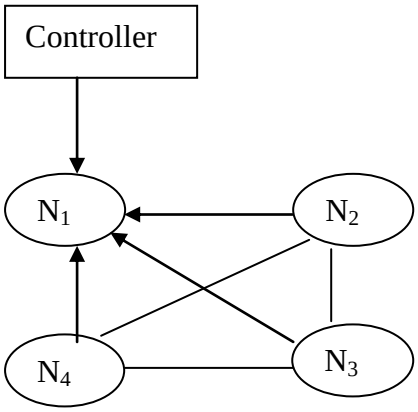

Fig-2: An AON with four nodes and a Controller

2.1. Attack Detection using Neural Network

At any given time, t, to detect whether an attack has been encountered by the optical node say, N_1, its neighbouring nodes N_2, N_3 and N_4 sends data packets at fixed rates. Each data packet send by its neighbouring node say, N_2, is considered to be an input say, I_1. A weight, W_1, is being assigned for the input, I_1. For each input data packet being send by N_2, if the data packet is received successfully within a specific time period then the weight assigned to it is 1 otherwise 0 is being assigned. Suppose 1000 data packets have been sent by the node, N_2, then for each packet received or not received, could be computed using the input function of the neural equation:

$$X = \sum_{i=1}^{n} W_i I_i + \mu_i$$

Where, I_i, is the data packet being sent and

W_i, is 1 if packet is received successfully, or

W_i, is 0 if packet is not received successfully and

μ_i, is termed as negative, if W_i is 0, otherwise is termed as positive, if W_i is 1.

The value of input function is evaluated and if it is seen that the computed value of X, is more than or equal to the fifty percent of the actual value of X being ideally computed, then it is stated that the attack is not encountered in the node, N_1. A packet is said to be successfully received by the node, N_1, if it properly acknowledges N_2 about the same within a specific time frame. So a timer is been initialized for each packet sent by the node, N_2, and it waits for a specific time period so that the acknowledgement is received within the specific time frame.

2.2. Attack Management using Greedy Algorithm

As soon as an attack is being detected by a neighbouring node say, here, N_2, it propagates this message to the Controller using Greedy algorithm. The Controller, on receiving the message of the attack at node, N_1, alarms all the neighbouring nodes of N_1 using the Greedy algorithm. Thus in both the cases, after an attack has been detected and the message has to be conveyed the same algorithm is been used. The Controller keeps a routing table in the form of a two-dimensional matrix where it stores the shortest routes to be traversed to reach a particular node. Once it receives an attack message from a node say, N2, it traverses the routes stored in the routing table so as to propagate the alarm to all neighbouring nodes. Once the alarm/attack message is received by each node, consequently the routes to the attacked node are avoided by them. The neighbouring nodes choose alternative paths to avoid the attacking node.

3. ATTACK DETECTION ALGORITHM

Step 1: Set up the mesh network.
Step2: Call subroutine init_network ().
Step3: Call subroutine get_node_info (). Get the nodes information.
Step 4: Call subroutine chk_fault (). Check the fault/attack in a node.
Step 5: Stop

Subroutine init_network ()

Step1: Accept the number of optical nodes in the network and assign the value in a variable called count.
Step 2: Initialize two variables i=0 and j=0 for at least two nodes to be present for a network.
Step 3: If the value of i is equal to that of j then network cannot be established.
Else, set up an adjacency value for connection from node I to node j. For direct connection, adjacency value is 1(non-zero) otherwise, 0.
Step 4: Set up the synaptic weights, W_{ij}, for connection from node i to j.
Step 5: Increment j by 1.
Step 6: If the value of j is less than count, then go to Step 2. Else, increment i by 1.
Step 7: If the value of i is less than count, then go to Step 2. Else, display the number of nodes in the network.
Step 8: Stop.

Subroutine get_node_info ()

Step 1: Input the reporting node's index as self_index.
Step 2: Input the checking node's index as chk_node_index.
Step 3: Input data packet transfer rate from the reporting node to checking node, which are acknowledged.
Step 4: Accept the value of data packet transfer rate in a variable called check. It is computed using the input function, of the ANN as follows:

$$X = \sum_{i=1}^{n} W_i I_i + \mu_i$$

Where, W_i is the synaptic weight of input data packet, I_i. W_i is 1, when data packet, I_i, is successfully received by checking node, otherwise, it is 0. The biased term, μ_i is negative for W_i equals to 0, else μ_i is 0.1.
Step 5: Assign the value of X to check.
Step 6: Stop

Subroutine chk_fault ()

Step 1: Accept the value of check from subroutine get_node_info ().
Step 2: If the value of the variable, check is more than or equal to fifty percent of the value of X, being ideally computed, then display message that no fault has occurred in the checking node. Display the checking node's index, chk_node_index. Else, display the message fault detected in the checking node. Display the checking node's index, chk_node_index.
Step 3: Inform the chk_node_index to the Controller.
Step 4: Stop

4. ATTACK MANAGEMENT ALGORITHM

Subroutine Controller ()

Step 1: Starting from the reporting node, initialize a variable, current = self_index.
Step 2: For each node, except self_index and chk_node_index i.e. attacked node, get the least adjacency value and the corresponding node, n.
Step 3: Inform the attack message to node, n.
Step 4: Assign the value of n to current.
Step 5: If all the nodes are informed then go to Step 6. Else, go to Step 2.
Step 6: Stop.

5. RESULTS AND DISCUSSION

The results of the proposed algorithm, its performance have been implemented on Pentium V machines using C as the programming language. The output shows the efficiency with and checks whether an attack has actually been encountered by any other node or node. Once an attack has been detected the message is propagated to the Controller, who conveys this message to all the neighbouring nodes. The result in the Fig. 5, shows attack being detected for network having 4, 6, 8, 10 and so on. The proposed algorithm has been tested on the NSFNET, Fig. 4 and the result shows that attack can be successfully detected.

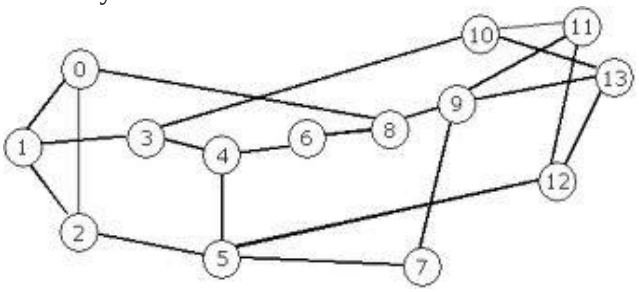

Fig-3: NSFNET

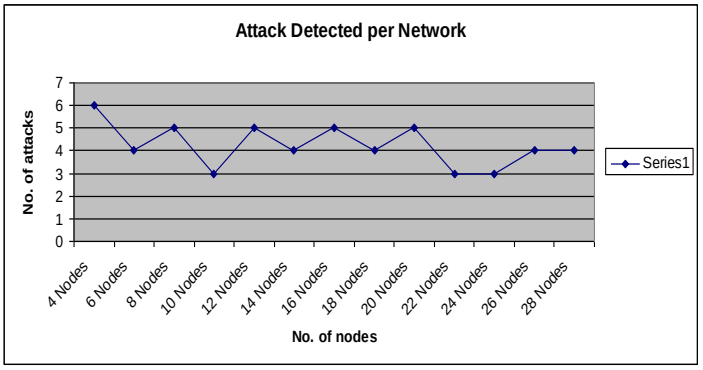

Fig-4: Results showing number of attacks detected as against number of nodes per network

6. CONCLUSION

This paper proposes two algorithms for attack detection and management in AON. The first algorithm detects attack using the concepts of ANN, where the input function is computed with the help of synaptic weights given to each such input. The resultant input function along with he biased term is used to determine whether an attack has really occurred on an optical node in a network or not. Based on some pre-assumed value of input function to be the idealistic value the computed value of input function is compared to detect whether an attack has been encountered by the node or not. Once the attack has been detected on an optical node, node which computes the attack in its first hand propagates the attack/alarm message to the Controller. The Controller conveys the attack message to all other neighbouring nodes which can be affected by the attacked node using the greedy algorithm. In this way, attack in a network could be detected and managed very easily.

ACKNOWLEDGEMENT

The authors of this research would like to thank B. P. Poddar Institute of Management and Technology for providing high-end computing laboratories during their research work.

REFERENCES

[1] Stamatios V. Kartalopoulos, Williams Professor in Telecommunications Networking,
"Optical Network Security: Countermeasures in View of Channel Attacks", Military Communications Conference, 2006. MILCOM 2006. IEEE , The University of Oklahoma, Washington, DC, ISBN: 1-4244-0617-X, pp. 1-5, Issue Date: 23-25 Oct, 2006.

[2] S.V. Kartalopoulos, "Fault Detectability in DWDM: Towards Higher Signal Quality and Network Reliability", IEEE Press, New York, NY, 2001.

[3] P.S. Andre, L.L. Pinto, A.N. Pinto, and T. Almeida, "Performance Degradations due to Crosstalk in Multiwavelength Optical Networks Using Optical Add Drop Multiplexers Based on Fibre Bragg Gratings", Revista Do Detua, Portugal, vol. 3, no. 2, pp. 85-90, Sept. 2000.

[4] S.V. Kartalopoulos, "Optical Network Security: Sensing Eavesdropper Intervention", Globecom 2006, San Francisco, on CD-ROM, NIS03-2, ISBN: 1-4244-0357-X, ISSN: 1930-529X.

[5] Stamatios V. Katalopoulos, "Discriminating between Faults and Attacks In Secure Optical Networks", Military Communications Conference, 2007. MILCOM 2007. IEEE , Orlando, FL, USA , ISBN: 978-1-4244-1513-7, pp.1-5, Issue Date: 29-31 Oct. 2007.

[6] Kartalopoulos, S.V. "Differentiating Data Security and Network Security", IEEE Communications, 2008. ICC'08. International Conference on Telecommun. Networking, Univ. of Oklahoma, Tulsa, OK, pp. 1469 – 1473, Issue Date: 19-23, May 2008.

BIOGRAPHIES

Inadyuti Dutt, has been in the field of academics and research for more than ten years and is currently the Assistant Professor in the Department of Computer Application of B. P. Poddar Institute of Management & Technology, Kolkata, West Bengal, India. .Earlier, she held several technical positions in National Informatics Centre, Kolkata and Semaphore Computing Networks Pvt. Ltd. respectively. She has earned Master's Degree in Computer Application and currently pursuing her research in Computer Science and Engineering. She has more than 15 publications to her laurels and her research interest is specifically in the field of Optical Networking, Security and Genetic Algorithms. She has also been Member, Editorial Board in journal publications like International Journal of Software Engineering & Research.

Soumya Paul, Assoc. Professor and Head, Department of Computer Application in B. P. Poddar Institute of Management & Technology, Kolkata, has been in teaching and research for over 12 years. He holds a Master's Degree in Technology, Computer Application as well as in Mathematics and has gathered vast experiences in the same. He received his M.Sc. (Mathematics) from Visva Bharati University and stood 1st class 1st. He received MCA from National Institute of Technology, Rourkella and M. Tech (CSE) from AAI-Deemed University and pursuing Ph. D in Computer Science and Engineering. He served as a faculty member and visiting faculty member in various Institutes and Universities like RCCIIT, Visva Bharati University, University of Calcutta, Bardhaman University, West Bengal University of Technology etc. He has delivered numerous lectures across India in the field of his research interest, Optical Networks and Genetic Algorithms. He is an author/co-author of several published articles in International Journals and International Conferences. He has chaired an International Conference technically supported by IEEE communication. He has more than 15 research publications and currently Reviewer and Member, Editorial Board in many conferences and journals like International Journal of Data Modelling and Knowledge Management.

Rahul Das is a software programmer presently, and working in Cognizant Technology Solutions. He is currently working on Mainframe Systems. He has completed his post-graduation from B. P. Poddar Institute of Management & Technology with 8.97 dgpa and has keen interest in research areas of security in optical networking. Apart from working in software industry, he is also involved in research activity in his domain.