ISSN No. 0976-5697

Volume 3, No. 2, March-April 2012

International Journal of Advanced Research in Computer Science

TECHNICAL NOTE

Available Online at www.ijarcs.info

Security in All-Optical Network using Artificial Neural Network

Inadyuti Dutt *and Soumya Paul
West Bengal University of Technology,
Department of Computer Application,
B. P. Poddar Institute of Management nd Technology,
Kolkata, West Bengal, India,
inadyuti@gmail.com, soumya.paul2000@gmail.com

Dipayan Bandyopadyay
GlobalIds Inc.,
Benfish Tower, GN-31, Sector-V,
Salt Lake City,
Kolkata, West Bengal, India,
nil007@gmail.com

Abstract: This paper concentrates on security attacks in All-Optical Network and proposes an algorithm based on the concepts of Artificial Neural Network. The algorithm uses the approach of artificial neurons where numbers of inputs are coupled with their assigned weights to produce an output of desired results. If the output matches a desired result then an internal optical node in a given network can be accessed by an external optical node. Here, the inputs are the external nodes' source ip-addresses, port numbers and response time in seconds as well as the internal nodes destination ip-addresses, port number and response time in seconds. The algorithm efficiently checks each of the input values assigned with weights and finally grants or forbid dens permission to the external node according to the computed output.

Keywords: All-Optical-Networks (AONs), Artificial Neural Network (ANN)

I. INTRODUCTION

Network security is an important component of All-Optical-Networks (AONs), as it is responsible for detecting attacks and preventing them at its first occurrence. Network attacks (commonly, termed as "hacks") can be classified in terms of Passive attacks and Active attacks. A passive attack usually tries to learn or make use of information from the system but an active attack attempts to alter system resources or affect their operations. Both these types of attacks are very difficult to detect. Passive attacks try to learn and make use of the information from the network whereas; the active attacks try to alter the network resources and their operations. Thus, active attacks must be detected as soon as an external agent or hacker tries to access the network or its resources. To do so a physical protection is required in all the communication facilities and paths at all times. The goal is to detect the active attacks at right time in the optical network and to prevent them from disrupting or delaying the normal functioning of the network. With the advent of new kinds of active attacks in AONs, more sophisticated techniques and methods are required to detect them. Artificial Neural Network (ANN) may be adopted to detect the dynamic behavior of such active attacks.

A. 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 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. The middle layer is the layer for processing unit, which takes inputs from the first layer. 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 particular , which normally are the same for all units within the whole ANN, i.e. the input function, processing unit 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:

$\text{Net}_i = w_{ij}\, x_{ij} + \mu_i$

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 is the 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.

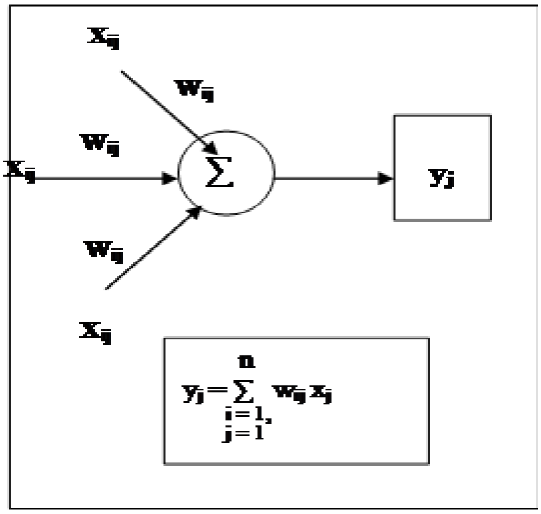


Figure: 1Mathematical representation of neural network

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.

B. 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:

a. Ability to learn:

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

b. 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 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 computes 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.

C. Outline of remaining sections:

The paper is organized as follows: Section II is the Body Text of the paper, which states the problem based on ANN technique in its subsection, A. The data structure, detailed description of the proposed ANN based algorithm with flowchart are described in the sub-sections of B whereas Section III shows the results and finally the paper concludes in Section IV.

II. BODY TEXT

A. Problem statement:

In this paper, 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 based on ANN uses this approach to detect any attack due to an external agent ("hacker"). An AON is considered to have several nodes each of them connected using a specific topology. The nodes are connected internally in either LAN or WAN. The ip-addresses of these nodes connected in LAN or WAN are known to each other. They belong to the internal network. When an external agent i.e., a node tries to acquire an access to the nodes which are internally connected then such type of illegal access is called an attack. These security attacks are prevalent in the AONs.

To detect such attacks in the network, an approach is considered using ANN where the multiple inputs such as ip-address of the external node, ip-address of internal node, port number to which the external node wants to communicate with that of internal node and time taken to establish the connection, are put together into the processing unit. Each such input has certain weight assigned to them and finally a numerical value, called bias is added to the computation. The output is a function of the weighted sum of the inputs plus a bias. So, an attack is said to be detected by an internal node as soon as the output function produces a result which is not acceptable. An alarm with a message is send to all other internal nodes stating the occurrence of an attack by an external node.

B. Proposed ANN based Algorithm:

a. Data Structure:

The data structures that are adapted for this algorithm are listed below

Assumptions: Consider an All-Optical-Network (Fig. 2) with N_1, N_2, N_3 and N_4 as its optical nodes. At any time, t, packets are send to an optical node say, N_1. N_1 encounters an attack by an external node say, N_6, not belonging to the assumed AON. N_1 belongs to the internal network and N_6 belongs to the external network.

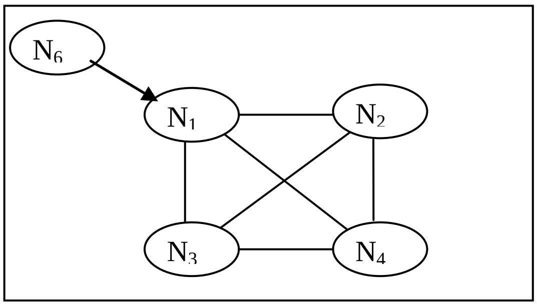


Figure. 2 An All-Optical-Network with its nodes

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

where, W_j =1, if the input (Ii) is valid
0, if the input is not valid
and,
I_i = 24, when the Source IP address is of Class A
I_i = 16, when the Source IP address is of Class B
I_i = 8, when the Source IP address is of Class C
I_i = 24, when the Destination IP address is of Class A
I_i = 16, when the Destination IP address is of Class B
I_i = 8 when the Destination IP address is of Class C
I_i = Source Port Number having range 0-65535
I_i = Destination Port Number having range 0-65535
I_i = Time Out value between 0-99999999
bias = A decimal error code value is added depending on the Error. 0 added in case of successful network connection. A connection to the network is successful if a valid external node wants to access a valid internal node.

$$X = \sum^{n} W_i I_i + bias$$

$i = 1$

N_1 is not attacked by the external node, N_6 if the value of X exceeds a given threshold value.

b. Description:

The algorithm starts with the initialization of each optical node with appropriate ip-addresses, port numbers and connection request availability time. These optical nodes are considered to be the internal nodes of the network. The optical nodes which do not belong to this network are said to be the external nodes to the network. The external nodes are also initialised with ip-addresses, port numbers and connection request availability time and connection timeout. Then an external node is randomly selected to get connected to an internal node. Both the selections of external and internal nodes are done randomly.

The internal node takes ip-address, port number and connection request time of the external node as inputs. With each correct source ip-address, a specific weight is multiplied with the input. Also, with each correct destination ip-address, a specific weight is multiplied with the input. Similarly, with each correct source port number to intended destination port number; specific weights are multiplied with these inputs.

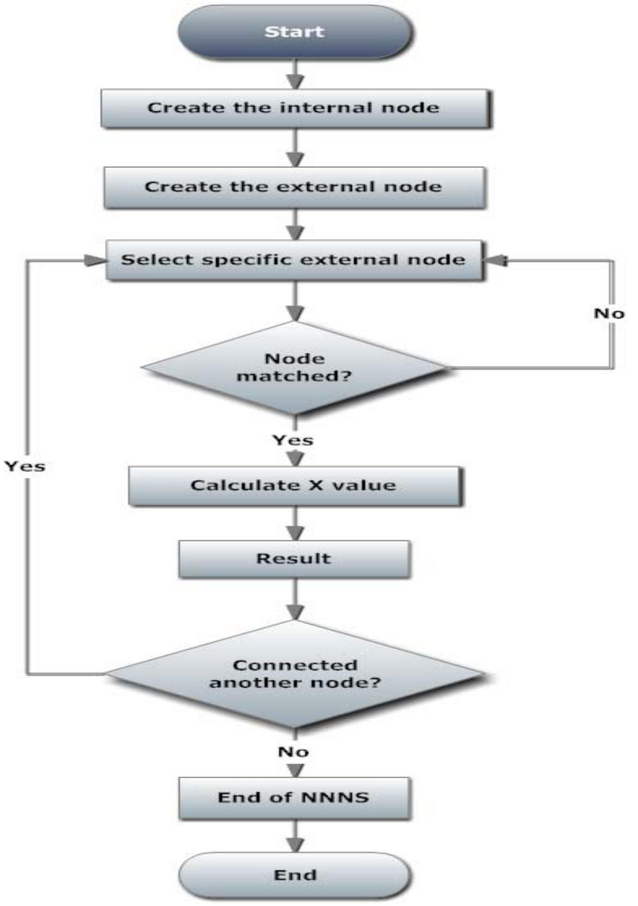


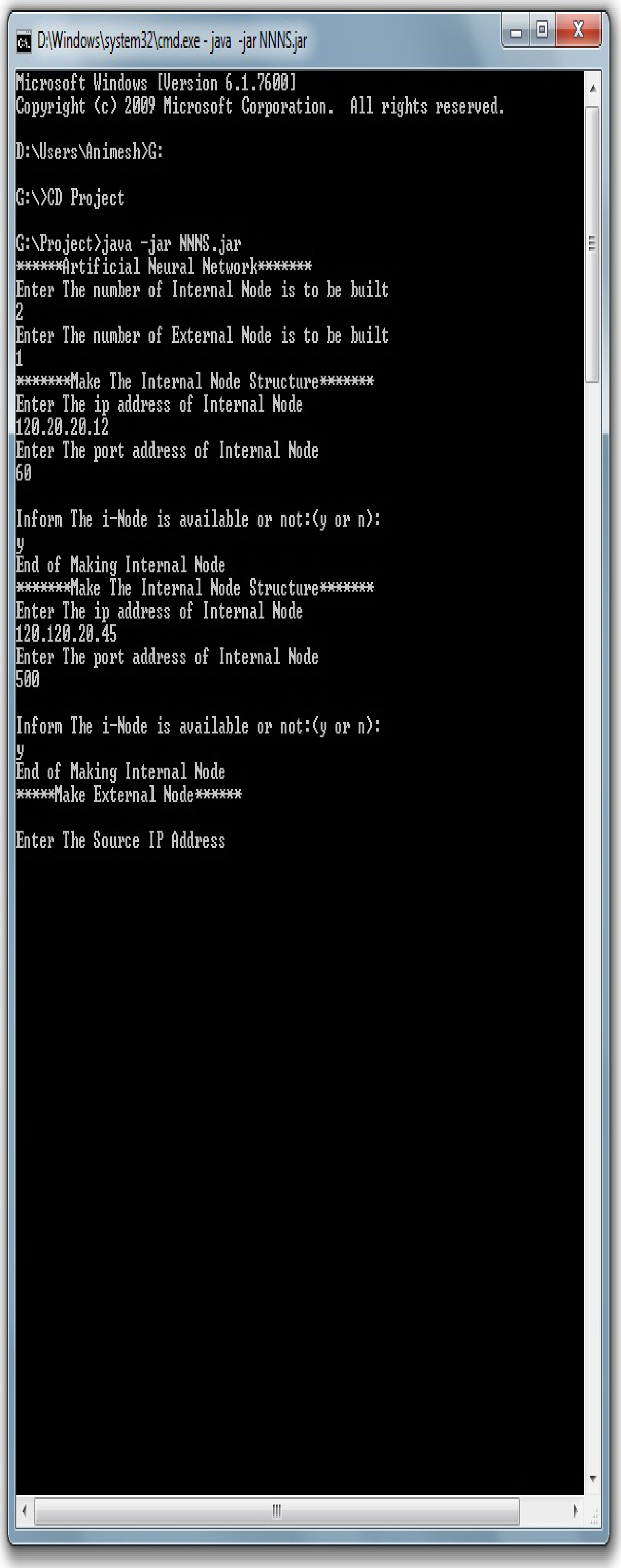
Figure. 3 Flowchart of the Proposed Algorithm

c. Proposed Attack Detection Algorithm

```
Step 1:
Make Internal Nodes which are Combination of IP address, port number and connection availability
Step 2:
Make External Nodes which are Combination of Source IP address, Destination IP address, Source Port Number, Destination Port Number, Connection Timeout and Connection Availability.
Step 3:
Select the specific external Node to be connected randomly.
Step4:
    If The Destination IP address of External Node matches with any of the Source Address Then
Then Goto Step 5
Else Goto Step 4
Step 5:
    Depending on $I_i$ sets of Internal and External Node, The weight is calculated.
$X = ((\sum^{n} W_j I_j) + \text{bias}$
Step 6:
Show the X or Result
Step 7:
If error_val =0 Then
    The External Node and Internal Nodes are valid nodes to be connected. External Node is not Hacker. They can be connected.
Else If error_val=.64 Then
    The destination port no of External Node does not match with the Port No of Internal Node
Else If error_val=.32 Then
    The Internal Port no of External Node does not match with the Port No of Internal Node
Else If error_val=.16 Then
    The Source IP address of External Class and The Destination IP address of Internal Class are not in same IP Class.
Else If error_val=.8 then
    If the Specified Internal and External Node don’t have The Connection availibilty
Else If error_val=.2 then
More than above errors have been occurred.
Step 8:
If user wants to connect another node then
If True then Goto Step3
Else
Goto Step 9
Step 9:
Stop / End.
```

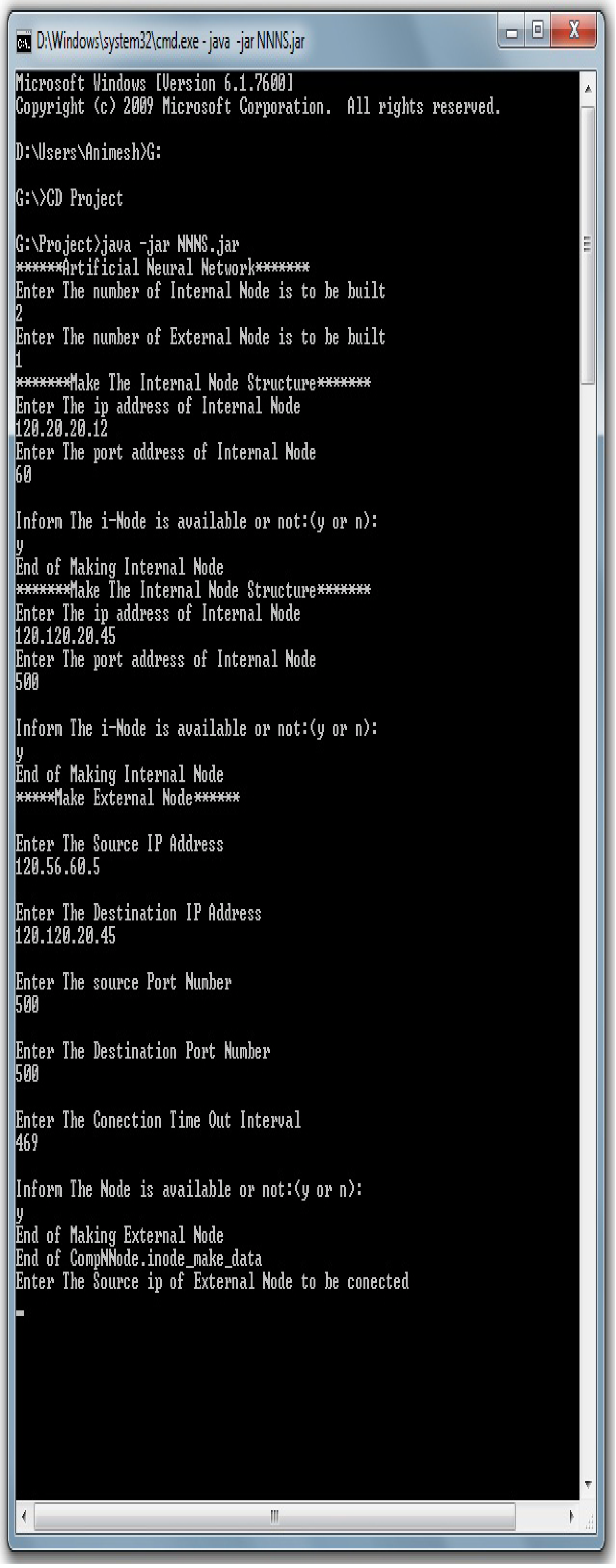
III. RESULTS AND DISCUSSION

The results of the proposed algorithm, its performance have been implemented on Pentium V machines using Java as the programming language. The output shows the efficiency with which the java code interacts with the internal nodes of a network and checks the validity of the external node for security attacks. At first the proposed algorithm initializes internal and external nodes and the network as given in Figures. 4 and 5. Then it accepts the ip-addresses of source and destination nodes with their corresponding port numbers to be connected respectively. Also it accepts the connection timeout and connection availability as inputs shown in Figures 6 and 7. A valid external node’s source ip-address and port number wishing to connect to a valid internal node’s destination ip-address and port number will produce no error. And Fig. 8 shows the either the denial or grant for permission to external node, which tries to connect with the internal node’s port.



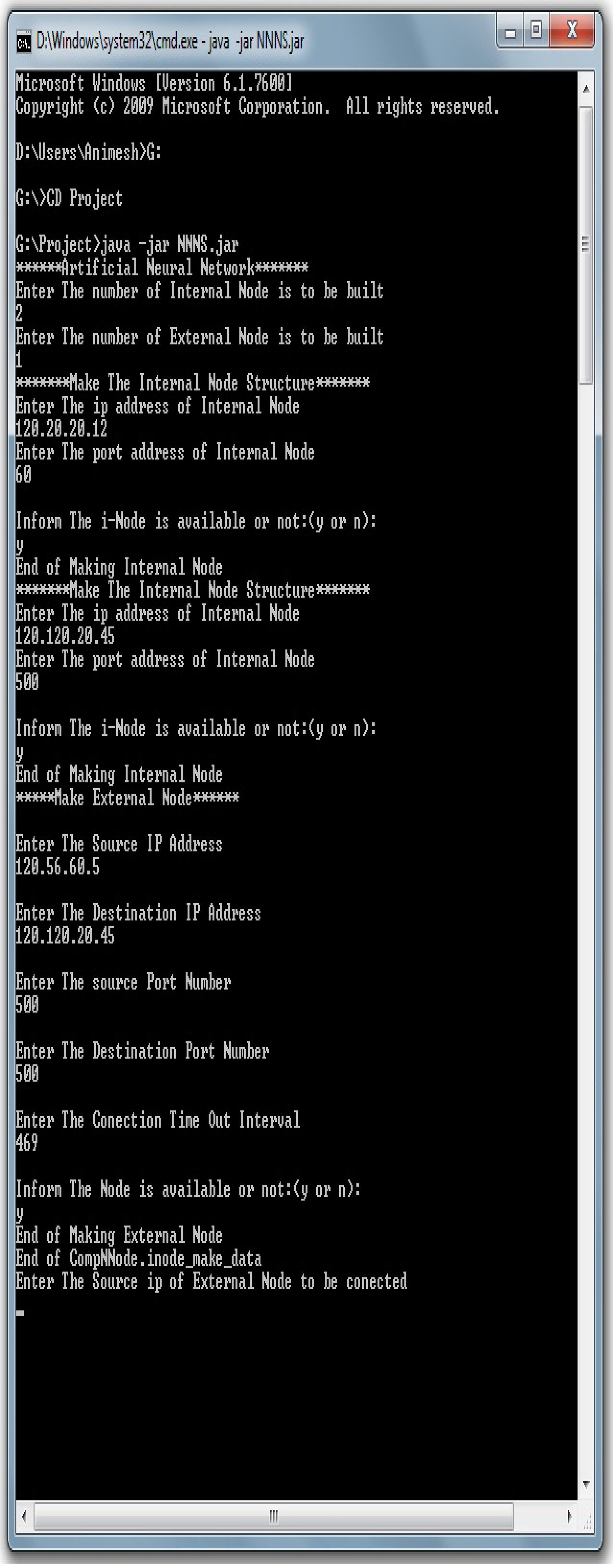
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

D:\Users\Animesh>G:

G:\>CD Project

G:\Project>java -jar NNNS.jar
******Artificial Neural Network*******
Enter The number of Internal Node is to be built
2
Enter The number of External Node is to be built
1
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.20.20.12
Enter The port address of Internal Node
60

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.120.20.45
Enter The port address of Internal Node
500

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*****Make External Node******

Enter The Source IP Address
```

Figure.4. Initialization of internal nodes of an Internal Network.



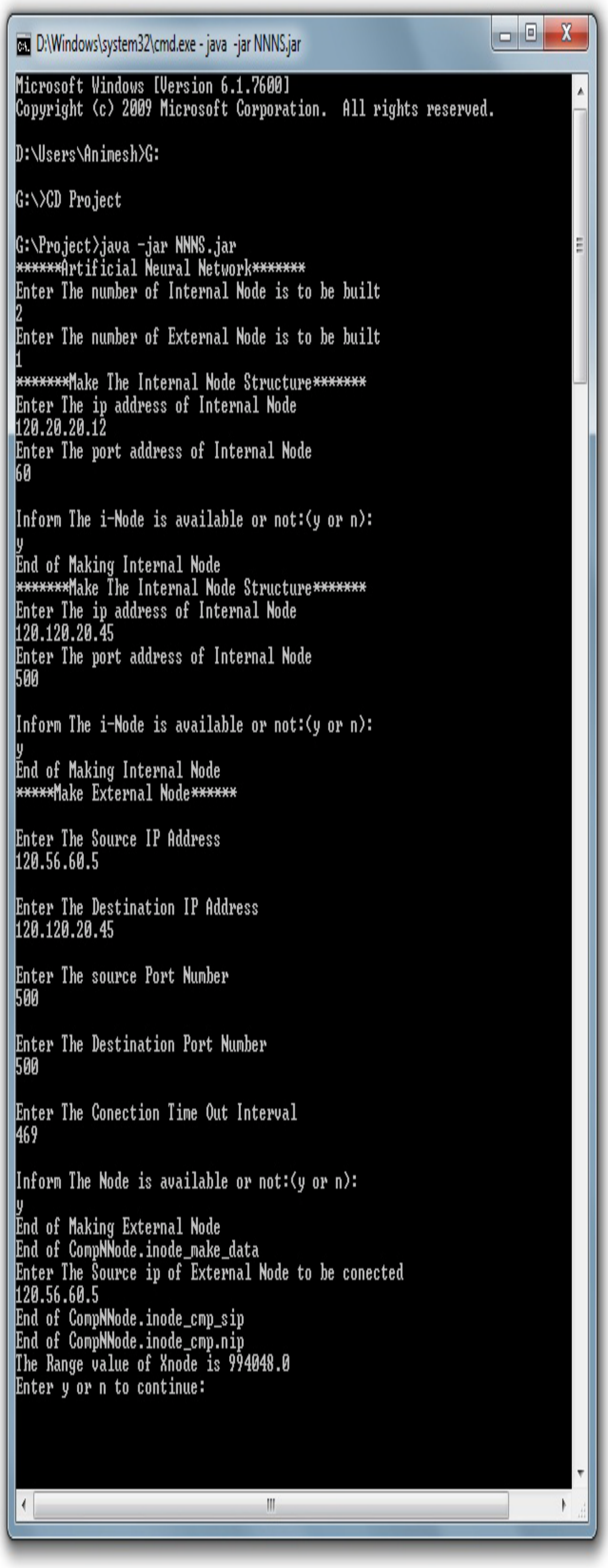
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

D:\Users\Animesh>G:

G:\>CD Project

G:\Project>java -jar NNNS.jar
******Artificial Neural Network*******
Enter The number of Internal Node is to be built
2
Enter The number of External Node is to be built
1
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.20.20.12
Enter The port address of Internal Node
60

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.120.20.45
Enter The port address of Internal Node
500

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*****Make External Node******

Enter The Source IP Address
120.56.60.5

Enter The Destination IP Address
120.120.20.45

Enter The source Port Number
500

Enter The Destination Port Number
500

Enter The Conection Time Out Interval
469

Inform The Node is available or not:(y or n):
y
End of Making External Node
End of CompNNode.inode_make_data
Enter The Source ip of External Node to be conected
```

Figure.5. Initialization of external nodes of an External Network.



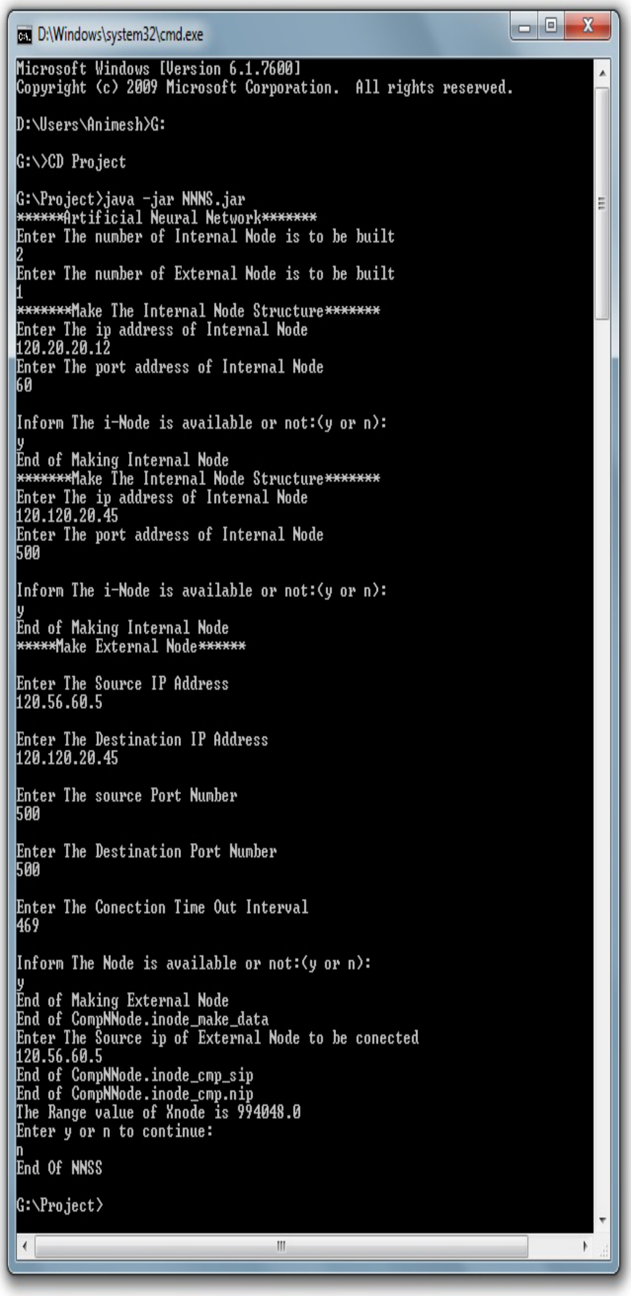
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

D:\Users\Animesh>G:

G:\>CD Project

G:\Project>java -jar NNNS.jar
******Artificial Neural Network*******
Enter The number of Internal Node is to be built
2
Enter The number of External Node is to be built
1
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.20.20.12
Enter The port address of Internal Node
60

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.120.20.45
Enter The port address of Internal Node
500

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*****Make External Node******

Enter The Source IP Address
120.56.60.5

Enter The Destination IP Address
120.120.20.45

Enter The source Port Number
500

Enter The Destination Port Number
500

Enter The Conection Time Out Interval
469

Inform The Node is available or not:(y or n):
y
End of Making External Node
End of CompNNode.inode_make_data
Enter The Source ip of External Node to be conected
```

Figure.6. Representation of the values taken from Source (External) Node.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

D:\Users\Animesh>G:

G:\>CD Project

G:\Project>java -jar NNNS.jar
******Artificial Neural Network*******
Enter The number of Internal Node is to be built
2
Enter The number of External Node is to be built
1
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.20.20.12
Enter The port address of Internal Node
60

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.120.20.45
Enter The port address of Internal Node
500

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*****Make External Node******

Enter The Source IP Address
120.56.60.5

Enter The Destination IP Address
120.120.20.45

Enter The source Port Number
500

Enter The Destination Port Number
500

Enter The Conection Time Out Interval
469

Inform The Node is available or not:(y or n):
y
End of Making External Node
End of CompNNode.inode_make_data
Enter The Source ip of External Node to be conected
120.56.60.5
End of CompNNode.inode_cmp_sip
End of CompNNode.inode_cmp.nip
The Range value of Xnode is 994048.0
Enter y or n to continue:
```

Figure.7. Representation of the values taken from Destination (Internal) Node.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

D:\Users\Animesh>G:

G:\>CD Project

G:\Project>java -jar NNNS.jar
******Artificial Neural Network*******
Enter The number of Internal Node is to be built
2
Enter The number of External Node is to be built
1
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.20.20.12
Enter The port address of Internal Node
60

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*******Make The Internal Node Structure*******
Enter The ip address of Internal Node
120.120.20.45
Enter The port address of Internal Node
500

Inform The i-Node is available or not:(y or n):
y
End of Making Internal Node
*****Make External Node******

Enter The Source IP Address
120.56.60.5

Enter The Destination IP Address
120.120.20.45

Enter The source Port Number
500

Enter The Destination Port Number
500

Enter The Conection Time Out Interval
469

Inform The Node is available or not:(y or n):
y
End of Making External Node
End of CompNNode.inode_make_data
Enter The Source ip of External Node to be conected
120.56.60.5
End of CompNNode.inode_cmp_sip
End of CompNNode.inode_cmp.nip
The Range value of Xnode is 994048.0
Enter y or n to continue:
n
End Of NNSS

G:\Project>
```

Figure. 8 Representation of the permission granted or denied depending upon the value of computed output.

IV. CONCLUSION

In this paper, an algorithm has been proposed and implemented for AON security attacks with the help of ANN concepts. The algorithm uses the approach of artificial neurons where numbers of inputs coupled with their weights come together into the processing element/unit and produces an appropriate output if and only if it matches a desired value. It uses the similar phenomenon by coupling all the inputs like source ip-address, destination ip-address, source port number, destination port number and response time respectively into the internal node and checks each one of its validity. The validity checking is done with some weights being assigned for each correct/incorrect input. If the inputs coupled with weights produce the desired output then the external node is allowed to access the internal node of the network otherwise a security attack is said to have occurred on the specific node.

V. ACKNOWLEDGMENT

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

VI. RESOURCES

Stamatios V. Kartalopoulos, ‘Optical network security: countermeasures in view of channel Attacks’, Military Communications Conference, 2006. MILCOM 2006. IEEE, 23-25 Oct. 2006, Pg. No. 1 – 5, 12 February 2007.

Stamatios V. Kartalopoulos, ‘Discriminating between Faults and Attacks in Secure Optical Networks’, Military Communications Conference, 2007. MILCOM 2007, IEEE, 29-31 Oct. 2007, Pg. No. 1-5, 22 February 2008.

VII. BOOKS

Rajasekaran S., Vijayalakshmi Pai G. A. ‘Neural Networks, Fuzzy Logic, and Genetic Algorithm Synthesis and Applications’. New Delhi, PHI Learning Pvt. Ltd., 2009.