CHAPTER 4

PROPOSED COGNITIVE FRAMEWORK ARCHITECTURE USING
BACK PROPOGATION ALGORITHM


The major objective of the undertaken work is to introduce security strategies with intelligent concepts like CSM, to provide security to network. CSM authenticates the user nodes for the grant of permission to access the associated network resources and other services, which is being achieved on the Physical hardware attributes of the nodes and behavior of the nodes in the network.

The work has been carried out on IEEE802.11 registered networks in the laboratory to study of standard security protocols. Security is provided to the WLAN, by making use of PADL, which is being used to authenticate the system that tries to access the wireless network by CSM. CSM maintains network integrity of all the nodes by observing their behavior. Figs. 4.1 and 4.2 illustrate the proposed cognitive wireless network and the conceptual architecture of CSM.
**The Process carried out by the CSM illustrated below steps**

**Step 1:** Whenever Wireless ad-hoc nodes enter into the wireless local area network environment, CSM records PADL of each node. It preserves the PADL attributes of each node, which is wishing to join the network.

**Step 2:** The CSM investigates the authentication of each node from the PADL repository. This repository is conserved by the CSM.

The PADL of the node and behavior pattern of the node are provided to the neural Network. The trained neural network assesses the node behavior. Operation of the CSM is explained by the below algorithm. The registration process of PADL which is carried out in this work prevents un-authorized admittance of nodes in to network, thus safeguarding security and integrity. The neural network based PM in CFA will identify the un-authorized network resource usage exhibited by the node thus providing security for the network.
The conceptual architecture consists of different functional units. CSM performs cognitive analysis and identifies the node based on PADL. PADL repository of Nodes, which houses two sections authorized and unauthorized sections. Authorized section is the collection of nodes which are authorized to use or access the network resources and other services. Unauthorized section is the collection of nodes which are deviated from network services access permission or privileges set by Administrator Tool Set. Administrator Tool Set imposes Network service access privileges to the node. It is also used to alter the CSM configuration whenever needed. The PM performs neural analysis to analyze the user node behavior to achieve cognition. PM houses both supervised and unsupervised learning algorithm based neural networks.
4.2. AC using PADL

When a node enters into the wireless environment under consideration, the CSM secures the network using AC and the cognition process as explained below.

**Step 1:** Accepts node’s PADL, which enters in to the existing wireless network environment and CSM relates the node’s PADL with in the PADL repository.

a) If a Node PADL is not found in the repository of PADL then it is treated as New Node. - Go to step 4

b) If a Node PADL found in the PADL repository then Investigate for the node status as an authorized or unauthorized

i) If node is authorized then - Go to step 2

ii) Otherwise node is unauthorized then - Go to step 3

**Step 2:** Behavior of the node in the wireless environment is observed, based on the network resource access privileges assigned by the network administrator go to step 5

**Step 3:** Network Service access is denied and go to step 7
**Step 4:** If new node then

c) Respective PADL of the new node is stored into the PADL Repository

d) Administrator will issue conservative Network resource or other services access permission to the new node.

e) This node is monitored under the established conditions.

**Step 5:** PADL and behavior patterns or characteristics of the nodes are fed into the neural network. Trained or skilled neural network frameworks estimate the behavior pattern of that node along with its respective PADL.

**Step 6:** Behavior of the node i.e., actual output is Compared with the estimated behavior, if it is found to be equal then node experiences uninterrupted service access permission.

**Step 7:** Behavior of the node i.e., actual output is Compared with the estimated behavior, if it is found to be unequal then CSM remove from the authorized register section and move the PADL of that node is transfer to unauthorized register section node experiences uninterrupted service access permission.
Figure 4.3 State diagram of Cognitive analysis carried out by the CSM

CSM - Security PM based on Neural Network

For the purpose of monitoring and analyzing the behavior of the nodes, Back Propagation Algorithm in cognitive approach has been implemented. The approach utilizes Multilayer Neural Network trained by Back Propagation algorithm with pattern wise learning stages. The neural network based security manager detects the illegal access of the network resources and service provisions. The qualified Neural Networks calculate deviation of node behavior from the skilled pattern or trained pattern.
4.3 Cognition Engine based on Back Propagation Algorithm

The projected Neural Network comprises of three layers, these are input, output and hidden layers which is illustrated in fig. 4.4.

![Back propagation based Neural Network diagram](#)

**Figure 4.4: Back propagation based Neural Network**

While in operation, the valid input which is derived from the registered node data transactions is fed to the input. The common operation homogenous pattern generated over a span of time will be consider as trained patterns and used to train the network. The security policy framed permits utilizations of network resources and other network services for user node. The difference in the operation patterns observed could be used to identify the malicious activities over PADL registered nodes by the neural networks. This decides the denial of permission to a particular node and subsequently removal of the same from authorized registered section to the un-registered section of PADL repository, thus the node experiences no access permission to use
network resources. The cognition process is realized based on the neural networks and its formulation is discussed below.

Input usage vectors have been provided at the input layer which is being broadcasted through the network and output vector appears at the terminating layer of the network. The error signal generated at the output layer is propagated backward through the network. The output layers consists of Number of output neurons represented as $c$, input neurons constitute input layer represented as $a$, one or more hidden layers present in between input layer and output layer and are consist of hidden neurons denoted by $b$.

The error signal computed at the output layer can be expressed as provided below

$$e_c(t) = d_c(t) - y_c(t) \quad \text{----- (4.1)}$$

Where

$e = \text{error signal obtained at output layer},$

$c = \text{Number of neurons considered in the output layer},$

$t = \text{number of iteration}$

Total error energy can be obtained by Equation 4.2 ,

$$\text{Total error energy} = \frac{1}{2} \sum e_c(t)^2 \quad \text{----- (4.2)}$$
This total error energy could be back propagated from output layer to input layer via hidden layer. Adjustment of weights and threshold at each layer could be carried out with this error. The purpose of adjusting both weights and threshold is to minimize the total error energy. The term called momentum $\mu$ which is used to control the adjustment cycle and also increase the learning rate $\eta$ of the neural network. The undertaken work used the momentum based weight adjustment and threshold adjustment.

The induced local field $V_c(t)$, $V_b(t)$, can be calculated as below

$$V_c(t) = \sum_{a=0}^{m} W_{ca}(t)Y_a(t) \quad \text{----- (4.3)}$$

$$V_b(t) = \sum_{b=0}^{m} W_{bc}(t)Y_b(t) \quad \text{----- (4.4)}$$

Where $m$=total no. of inputs applied to $c$ neuron. Net output can be computed as below

$$y_c(t) = f(V_c(t)) \quad \text{----- (4.5)}$$

Error calculated at the output layer is

$$\delta_c(t) = y_c(t) \cdot (1 - y_c(t)) \cdot (d_c(t) - y_c(t)) \quad \text{----- (4.6)}$$

Error calculated at the hidden layer is
\[ \delta_h(t) = Y_h(t) (1 - Y_h(t)) \sum_{C=1}^{M} W_{bc}(t) \delta_C(t) \]  

----- (4.7)

Weight adjustment between output layer and hidden layer

\[ \Delta W_{bc} = \eta \delta_C(t) Y_h(t) \]  

----- (4.8)

Weight adjustment between hidden layer and input layer

\[ \Delta W_{ab} = \eta \delta_h(t) Y_a(t) \]  

----- (4.9)

Where Change or Adjustment in synaptic weight is represented by \( \Delta W \), \( \eta \) is represented as learning rate. The local gradient is represented as \( \delta_c(t), \delta_h(t) \)

Momentum is magnitude of the perseverance. The weight update, threshold update are calculated using momentum term as below

\[ \Delta W_{bc} = \eta \delta_c(t) Y_h(t) + \mu \Delta W_{bc} (old) \]  

----- (4.10)

\[ \Delta W_{ab} (new) = \eta \delta_h(t) Y_a(t) + \mu \Delta W_{ab} (old) \]  

----- (4.11)

Threshold update

\[ \Delta \theta (new) = \eta \delta_h(t) + \mu \Delta \theta (old) \]  

----- (4.12)
Figure 4.5 Flow Chart of the Proposed System Processing

START

NEW NODE

Deposit the PADL into the PADL Repository. Obtain its service access permission from the administrative tool set. Grant service access permission under monitored conditions.

NODE Ni ENTERS THE WLAN

EXTRACT PADL & CHECK IN PADL REPOSITORY

AUTHORISED

Obtain behavior characteristics of the nodes and provide the PADL of the node to the neural network as an input. The trained neural network framework estimates the behavior pattern of the node with respect to its PADL.

If the behavior of the node
—
neural network based estimated behavior,

the node observes uninterrupted service access permission

Move the PADL to Un-Authorized section in the PADL

STOP

Then the service access permissions are withdrawn.
4.4 **Experimental Evaluation and Observations.**

It is very much essential to evaluate the Cognitive Frame work Architecture based on the CSM, where in the required security to the WLANs are provided by the CSM using two mechanisms, which are

1. AC using PADL
2. Cognition Engine based on BPNN

AC mechanism needs to be swifted, easy and requires having minimal user interaction. This mechanism using PADL needs to be evaluated ensuring that Cognition has been achieved by studying the user transactions on the network. The intelligence of understanding the user transactions is being achieved by using BPNN.

The wireless test bed consists of fifty varied configured desktops, three Quad Core Servers and multiple Laptops used at scheduled timings. The units under test were wirelessly linked through a number of APs. In order to achieve this objective Cisco’s Linksys WRT54G wireless router was used for better connectivity. The CSM is executed on the 4 GB RAM with Quad Core Server of Intel.

The PADL extraction is a key feature of the cognitive framework, where in PADL is a combined description of the physical layer of the user nodes.
A C++ library was developed to extract the PADL of the user nodes and is integrated into a C# based graphical user interface.

A sample PADL Extracted is shown below

Operating System
--- Version: 5.2.3790
--- Manufacturer : Microsoft Corporation
--- Computer Name : THINSERVER
--- Windows Directory : C:\WINDOWS
--- Serial Number : 6971.3-640-5167547-45328

Computer System
--- Computer Manufacturer Name: Intel
--- Computer Model : SBR20
--- System Type : X86-based PC
--- Total Physical Memory: 1,048,048 KB
--- Domain : knsit.com
--- User Name : THINSERVER\Administrator

System Processor --- Manufacturer : GenuineIntel
--- Computer Processor : x86 Family 15 Model 2 Stepping 7
--- CPU Speed : 1.794GHz
--- L2 Cache Size : 1 KB
--- Manufacturer : GenuineIntel
--- Computer Processor : x86 Family 15 Model 2 Stepping 7
--- CPU Speed : 1.794GHz
--- L2 Cache Size : 1 KB
--- Manufacturer : GenuineIntel
--- Computer Processor : x86 Family 15 Model 2 Stepping 7
Figure 4.6 Extracted PADL

The PADL as shown above is comprehensive and contains multiple data about the hardware layer of the user nodes and this becomes the identification of the user nodes in the network. PADL Extraction should
not burden the network performance and the extraction process should be quick.

\[
PADLEXTRACTIONOVERHEAD = \frac{(StopTime - StartTime)}{ProcessorFrequency} = \frac{t_{stop} - t_{start}}{f_{Processor}} \quad \text{..... (4.13)}
\]

Here PADL extraction overhead is calculated with system clock and processor frequency.

In order to evaluate the effect of PADL extraction on user nodes a methodology shown through the above equation is established to extract the PADL from the user nodes of the designed test bed setup and the results are tabulated as shown in the Table 4.1. The processor frequency is obtained using the operating system kernel files (For Windows based systems it is Kernel32.dll).

**Table 4.1: Node Specification versus Average PADL Extraction Time**

<table>
<thead>
<tr>
<th>Node Specification</th>
<th>Average PADL Extraction Time in ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop – AMD Processor</td>
<td>3.1826</td>
</tr>
<tr>
<td>Desktop- Intel P4 Processor</td>
<td>1.8860</td>
</tr>
<tr>
<td>Server- Intel Quad Core</td>
<td>5.4109</td>
</tr>
<tr>
<td>Laptop-Dell Intel Centrino</td>
<td>3.0058</td>
</tr>
<tr>
<td>Laptop-Acer Dual Core</td>
<td>3.4407</td>
</tr>
<tr>
<td>Laptop- Sony Vaio Core2 Duo</td>
<td>3.3402</td>
</tr>
</tbody>
</table>

The average PADL extraction time across varied platforms is about 3.377 ms. The PADL could be extracted very quickly and does not
burden the user system. The average size of the PADL is about 2 kilobytes. The PADL extracted is sent as a file to the CSM maintained on the server. The PADL transactions between the user and the CSM were found not to affect the network performance due to their negligible size.

Classification of the nodes into authorized and unauthorized nodes is very critical and the first important function of the CSM is to realize writing an application using C# as the programming language. The CSM was installed on an Intel Quad Core Server. The CSM which houses the PADL repository of nodes was populated width 60, 80, 100, 120 and 140 PADL of user nodes. The nodes were equally distributed into authorized and unauthorized nodes. The node is classified as a new node if it is not present in the PADL repository. The response times of the CSM were recorded and the tabulated data is provided below.

**Table 4.2: Response Time of CSM**

<table>
<thead>
<tr>
<th>Number of PADL in the repository</th>
<th>Response Time for Authorized Node in (ms)</th>
<th>Response Time for Unauthorized Node(ms)</th>
<th>Response Time for New node in(ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>0.07637</td>
<td>0.12984</td>
<td>0.1992</td>
</tr>
<tr>
<td>80</td>
<td>0.15472</td>
<td>0.14826</td>
<td>0.2230</td>
</tr>
<tr>
<td>100</td>
<td>0.17913</td>
<td>0.16055</td>
<td>0.2360</td>
</tr>
<tr>
<td>120</td>
<td>0.21632</td>
<td>0.22035</td>
<td>0.2556</td>
</tr>
<tr>
<td>140</td>
<td>0.26231</td>
<td>0.23372</td>
<td>0.3188</td>
</tr>
</tbody>
</table>

The response time of the CSM in node identification and classification as authorized, unauthorized and node is calculated and is shown in the
graph Fig. 4.7. CSM classifies the node and if it is an authorized node then it analyses its behavior pattern. For the process of analyzing behavior patterns of nodes, the CSM uses the back propagation algorithm.

**Figure 4.7: Graph of CSM Node Classification Analysis**

It is clear from the Table 4.2 that, response time of the CSM is directly proportional to nodes in the PADL repository. CSM Response time is increased with increase in nodes in PADL repository. The time taken to identify the new nodes takes more time when compared to authorized and unauthorized nodes. The response time of the CSM for node identification and classification is also acceptable. For 140 nodes the response time is below 0.31ms. After reviewing the CSM node classification behavior and it is now essential to observe and review the response of the CSM in analyzing the behavioral patterns of the nodes. It does the neural analysis based on the Back Prorogation Algorithm.
To evaluate the cognition engine the user nodes were monitored and their network transactions were studied. These transactions were provided as an input to the CSM. The neural network trained using back prorogations were used to analyze these transactions.

For the purpose of training the neural network a conservative transaction set also called as the administrative tool set is used for new nodes and the previous transaction was used for authorized nodes. For evaluation, transaction sets varying from 30, 40, 50, 60, 70, 120 and 140 nodes were considered.

If an authorized node exhibited valid transactions the detection time was noted. If valid nodes exhibited invalid transaction the detection time was calculated and for new nodes their network transactions too were studied. The detection of the transaction and the CSM response times are tabulated as illustrated with the below table 4.3.

**Table 4.3: Detection of Transaction versus Training set**

<table>
<thead>
<tr>
<th>Training Set</th>
<th>Valid Transaction Detection Time</th>
<th>Invalid Transaction Detection Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>140</td>
<td>0.00264</td>
<td>0.00211</td>
</tr>
<tr>
<td>120</td>
<td>0.00214</td>
<td>0.00226</td>
</tr>
<tr>
<td>70</td>
<td>0.00224</td>
<td>0.00208</td>
</tr>
<tr>
<td>60</td>
<td>0.00222</td>
<td>0.00213</td>
</tr>
<tr>
<td>50</td>
<td>0.00221</td>
<td>0.00199</td>
</tr>
<tr>
<td>40</td>
<td>0.00221</td>
<td>0.00209</td>
</tr>
<tr>
<td>30</td>
<td>0.00249</td>
<td>0.00203</td>
</tr>
</tbody>
</table>

The detection of the CSM is shown in the graph indicated in Fig 4.7.
Figure 4.8: Graph of CSM Detection Time for Node Transaction Analysis

It could be analyzed from the observations that the response of the CSM to classify the transaction is quick and the back prorogation neural network based cognition engine is agile and fast to counter malicious network transaction of nodes. In case of detection of invalid transactions the CSM moves the node from the authorized to the illegal section of the PADL repository and unauthorized node experiences no service access permission to access network service and resources.