RESEARCH ARTICLE

Development of Hybrid Cognitive Security Managers on Improved Multilayer CFA Feed Forward Neural Network to Improve the Security on Wireless Networks

Senthil Kumar S
Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Tiruchirappalli, India.
✉ szenthilkumar@gmail.com

Suganya J
Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Tiruchirappalli, India.
suganyajeya2011@gmail.com

Kanagalakshmi K
Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Tiruchirappalli, India.
kkanagalakshmi@gmail.com

Hariharan C
Department of Management Studies, Faculty of Science and Humanities, SRM Institute of Science and Technology, Tiruchirappalli, India.
harisraj7791@gmail.com

Received: 02 January 2024 / Revised: 11 April 2024 / Accepted: 07 May 2024 / Published: 30 June 2024

Abstract – Wireless Local Area Networks (WLANs) that are currently deployed are vulnerable to assaults. The wireless networks have been secured with the application of cognition. A variety of soft computing methods can be utilized to accomplish cognition, whereby they are employed to supply the intelligence required to comprehend user nodes' malevolent actions. The consumer nodes activities are inherently dynamic. The strategies for autonomous protection and adaptation of the Wireless Network environment are investigated as a result of basic weaknesses within the IEEE 802.11 Access Control (AC) mechanism. In the cognitive framework architecture, an Improved Multilayer CFA (Color Filter Array) Feed Forward Neural Network (IMCFFNN) proposed to generate node behaviour patterns and then to analyze them using supervised multilayer CFA feedforward neural networks. The Cognitive Security Managers (CSM) can attain Cognition because the multilayer neural networks are efficient at detecting variations in user node behaviors. The CFA uses the Physical Architecture description layer (PADL) to identify nodes. A solid and effective framework has been developed from this work. Therefore, experiments have proved that malicious node behavior can be detected with 99 % effectiveness. In comparison to unsupervised teaching methods, similar rates of 94% are seen in the laboratory.

Index Terms – Wireless Local Area Networks, Cognitive Framework, Improved Multi-Layer Feed Forward Neural Network, Security, Performance Measures.

1. INTRODUCTION

Wireless networks, which provide a wide range of choices for integrating various communication systems smoothly, are helping to run the economy. The fact that the information is transmitted by air and poses a risk also raises security concerns for wireless networks [1]. An Access Point (AP) is part of the connection between a networks that consists of wired as well as Wireless networks. A significant security challenge is present in today's generation of wireless APs, which are designed to protect internal resources from external attacks. According to the relevant documents provided by the supplier, a large number of enterprises claim that security measures against unauthorized access and exploitation for APs are acceptable [2].

In the past ten years, there has been a marked increase in wireless LANs because they allow access to networked resources at anytime from anywhere. Moreover, it offers a wide range of services such as Internet connection which is often differentiated by its affordability, portability, and the fastest data transfer speeds. In contrast, studies are being conducted to protect WLANs and improve their reliability and security. WLANs are plagued with security issues, and one of the most important factors that prevent them from being secure is their difficulty in making it easy to establish adequate and effective security mechanisms [3].

The objective of the research project is to create a mobile security architecture that will address shortcomings in existing cellular deployment. Through the use of soft computing techniques, it has been able to deliver cognition. To achieve security, the proposed architecture relies on cognitive techniques and AC mechanisms [4]. Since the AC mechanism uses PADL and Cognition, brain networks and fuzzy rules have been applied to improve awareness, self-management, or coping with stress. Efforts were made to achieve a better structure and management of wireless networks, which indicates that they are not performing as well or the quality of service is poor [5].

All organizations have been forced to embrace Information and Communication Technology (ICT) as technology is increasingly advanced in today's world. Consequently, if the ICT system's security is compromised, all actions are directed through that system and an organization may be at risk of being penetrated. The need therefore for a heterogeneous system of detection and protection, capable of detecting truly innovative security threats as well as adapting itself to the new input needs to be addressed [6].

Two of the many systems that can be used to secure this information and ICT systems against vulnerabilities are anomaly detection and IDS. A drawback of anomaly detection systems is that it can be difficult to establish rules [7]. To ensure that the analysis is accurate, each process to be analyzed must be designed, implemented, and verified in addition to the risk inherent in detecting anomalies, it is also a failure to detect hazardous activity that complies with common use patterns. Therefore, a system of IDS which is both adapted to the latest innovative threats and able to train and implement using datasets with irregular distribution becomes essential [8].

This led to the emergence of a new era in networking, called cognitive networking that takes into account perception aspects such as learning, adaptation, goal setting, and optimization. The study and analysis of existing research proposals, which have been pointed out in the literature, have led to the design of an envisaged Community Network architecture that can be used according to specific CN methodologies [9]. A discussion and analysis have been conducted about the main elements of Cross Layer design for CNs and related placement problems, which have resulted in quantified results. The security method is assessed based on valid user identification to be able to achieve a particular objective. Since the information was monitored, there were concerns about data protection. The challenge of ensuring information security is, however, becoming more pronounced as the ICT management systems continue to grow in strength and technology advances. The entire system may be in danger and could have serious consequences if there were a breach of information security [10].

In this context, it is considered a security concern to preserve the privacy of network communications. For the record, only the intended recipient is capable of intercepting and reading messages transmitted to him or her over a secure network. As a result, it is necessary to ensure that information is protected from any infringement which might damage its confidentiality. Confidentiality may be threatened when information is shared with people who are not supposed to have it [11].

1.1. Motivation

Vulnerability in these WLANs poses a serious threat to network integrity. Current deployment technologies of access controls on wireless WLAN include MAC filter, Internet Protocol WPA, WPA2, and WEP. It would be easy to ignore the base filtering and a few other security measures and leave the WLAN unprotected [12]. The behavior of user nodes was assessed based on simplified computing techniques.

As a result of their ability to monitor node behavior in the network and take this knowledge into account for drawing up usage patterns by analyzing, convergence networks or CNs are also called 'smart networks'. Based on the composition of the use, the subsequent response measures were implemented [13]. It is from a Cognitive Process (CP) that CNs are realized. There is a growing research interest in cognition, and numerous techniques are being suggested to achieve it.

The cognitive engines provide the intelligence necessary to understand and observe the behavior of network conditions to acquire cognition through the use of estimation, game theory, evolutionary computation, fuzzy logic, Markov decision models, pricing theory, theory of social science, and reinforcement laws.

To achieve cognitive abilities, several researchers suggest the use of advanced computational techniques like genetic methods. In the suggested study, IMLFFNN is employed to achieve cognition through the application of neural network ideas. Neural network-based back propagation learning is incredibly effective [14].

1.2. Objectives

The objectives of the project are to secure wireless LANs by using AC mechanisms and cognitive techniques. The objectives of the research project are to set up a CFP framework, which is founded on CSM for developing smart wireless LANs. It is determined that CFA is embedded with both cognition engines and AC processes.

This paper is organized with six sections. In section 2, the related works and the literature survey are presented. The proposed IMCFFNN method is discussed in section 3. The description of the methodology is presented in section 4. The results and discussions are highlighted in section 5. The section 6 concludes the research work.

2. RELATED WORK

The IEEE 802.11 Wireless Communication Protocols are defined to allow wire-free communication between networks. Wireless networking is growing in conjunction with the Internet as wireless WLANs allow users to easily access any network from wherever they are. This enables us to combine the various telecommunications technologies in a seamless manner, which is good for the economy's functioning. In contrast, there is a great deal of difficulty in providing security on wireless networks [15].

The main challenge is the transmission of information by air. The authenticator is called the access point, which acts as a network intermediary between cellular and wired networks. The Associated Press raises more serious security concerns [16]. Wireless technologies like WLAN were rapidly developed in a short period. The reasons for this appeal are affordability, elasticity, simplicity of scalability. Wireless technologies have several important issues, such as security and poor QoS [17].

The deployment of WiMAX access points cannot prevent unauthorized entry and use. To meet the security objectives, including confidentiality, authentication, and authorization controls, many safety measures have been proposed [18]. The IEEE has been developing many standards for the transmission of voice and data over cellular networks. IEEE 802.11 is one of those crucial standards. A wireless LAN is the replacement for cabled networks. The two types are ad hoc mode and infrastructure mode. It is for this purpose that infrastructure modes are to be discussed. In this mode, wireless stations and APs communicate with each other via a wireless connection. WLANs are set up because the AP is attached to a wired network [19].

The three stages involved in establishing a connection between APs and stations are discovery, authentication, and association. The probe station is a facility that allows active and passive listening. During the authentication phase, the station shall be authenticated by the AP. The AP has just been sent a request from the station. After approval, the Associated Press adds a station to its table. The security of WLANs is compromised because they use radio frequencies for transmitting communications in the air Therefore, there is a problem with man-in-the-middle attacks and eavesdropping [20]. It's not an issue because wired networks have electrical wires attached to them for transmission. The objective of security is to achieve three things: integrity, secrecy, and authentication. One definition of confidentiality is the hiding of sensitive information during station-to-AP communication. In doing so, you prevent other users from hearing the conversation. Integrity means that the data being transmitted between the AP and the station is kept accurate. The security issues grow with the number of APs in the network as well [21].

Denial of Service (DoS) attacks have the greatest risk to wired and wireless networks. Access to wireless WLANs shall be restricted or permitted at a low data rate due to interference by external RF sources in the frequency spectrum. Another method of limiting access is to overload AP with alerts on Association failure which prevents other stations from joining them. Researchers have added other components to the Network in order to prevent such an attack, like the admission controller and global monitoring (GM) [22]. Researchers added further network components, such as admission control and Global Monitoring GM, for the prevention of this attack. These components establish a certain amount of bandwidth to use for the stations. packets that are affected by high traffic levels may be diverted to other APs to prevent DoS attacks. To detect statistical anomalies, it was proposed to use recurrent neural networks and to evaluate how well neural network architectures worked when used with the datasets from four different scenarios [23].

However, the KDDCup'99 data set remains an important benchmarking resource for assessing different methods of intrusion detection that can be used by the general public despite several problems in this area. The fact that machine learning approaches can cope with increasing complexity and a variety of threats is the main reason why they are so attractive. The existence and absence of the category were first determined, using a PN rule approach derived from P-rules and N-Rules, respectively. This is enhanced by the increasing detection rate of other types of assault, except for U2R [24].

Convolutional Networks Neural networks, which use the influence of biological factors, are an extension of traditional feed-forward networks FFNs. CNN was processing the images in their earliest versions with pooled 2D, fully aligned layers as well as a standard 2D layer. To evaluate the applicability of CNN for IDS and compare results with several cutting-edge techniques, the KDD Cup dataset from '99 was used. After a thorough investigation, CNN is better than all of the algorithms. Using an identical dataset, [25] studied how to use the Long Short-Term Memory (LSTM) classifier. Some believe that the LSTM's capacity for time travel and correlation of consecutive connection records is enough to make it a good fit for an IDS.

This effort aims to exploit the potential that incoming cyber-attacks may be unpredictable, and invisible to humans but manageable by placing an artificial intelligence layer on the network. Therefore, to be able to quickly identify a new attack and alert the system or initiate a preprogrammed response that may stop it from being continued, the neural network can be cultivated with available cyberattack data [26]. Therefore, by only adding layers to the security system, millions of dollars' worth of aftershock collateral damage and costly data leaks can be avoided. Due to the lack of benchmarking data available on network training, more recent data must be used before deployment in this field. This improves the robustness of an algorithm in real-time. The paper's primary aim is to integrate AI networks in a fast-emerging area of cyber security [27].

There have been frequent changes in the requirements and conditions for using or gaining access to network services. The transformation of the paradigms relating to networks, infrastructures, and access has led to considerable change as a result of Wireless Communication. Technology advancements enabled networking to be available wherever and at any time thanks to secure communications. This innovation is hampered by barriers such as a lack of security, reliable networks, and mobility support in Internet design [28]. The CN is a commonly used element for 4G wireless networks. A network's cognitive capacity is based on its understanding of its operating environment and its ability to adapt its operational variables to meet its tasks. The identification of a CP, or changes in working conditions and customer needs shall be one of the duties. Network elements such as base stations, switches, and routers shall be used to provide this service. Another name for CN is the 4G wireless network component [29]. The ability of a network to recognize its operating environment and modify its operational parameters to complete tasks is known as cognitive networking. The tasks involve identifying CP, or changes to the operating environment and user requirements. It requires provisioning from network components including switches, routers, and base stations.

They are in charge of hosting the ongoing tasks needed to complete the measurements needed for the reconfiguration of the network. The characteristics relate to active networks, which are distinct from CN networks and do not include CP. CN operates based on user objectives. The goals of each network element are directly related to the operation of the CN. CN operates within the confines of a data flow, which may comprise multiple network parts. When a single network element is subjected to high traffic or data flow, the CN makes decisions depending on the priority of these flows [30]. CN engages with the SAN to maintain a set of endpoint objectives, namely trust management, connectivity, and routing optimizations so that it can change parts of the SAN according to its requirements. The node is responsible for the network's overarching objectives in some defense and corporate networks. This makes it more likely that a node will shift from its own needs and that it will diverge from a profitable ISP and WAN, in which it is engaged in self-centered, local optimization operations. To achieve network-wide objectives, state information must be sent across nodes, which is critical to reducing overhead and complexity [31]. By demonstrating the level of difficulty and state information necessary to meet the objectives of the CN, the cost of anarchy serves as a director of the expansion of the CN.

This study investigated the amount of bandwidth to be used by the stations and the Packets that are experiencing a high traffic rate can be rerouted to nearby APs to prevent DoS attacks. The existing shortcomings are addressed by the proposed method for the effective and secured communications with an association of Feed Forward Neural Network.

3. PROPOSED METHOD

The input layer has complete connectivity of neurons with the hidden and output layers. The proposed CSM with IMCFFNN network architecture uses a system called the Backpropagation mechanism. The recommended architecture covers dropouts, bias, and full connection layers to increase network resilience is shown in Figure 1.

The proposed architecture for each application scenario is shown in Figure 2. Input and concealed layers: There are 41 neurons in this layer. The hidden layers then get these. ReLU is the non-linear activation function used in hidden layers. Regularization: To expedite and streamline the process, Dropout (0.01). Droppings provide a random disconnection of neurons, strengthening the model and preventing it from being overfitted with training data.

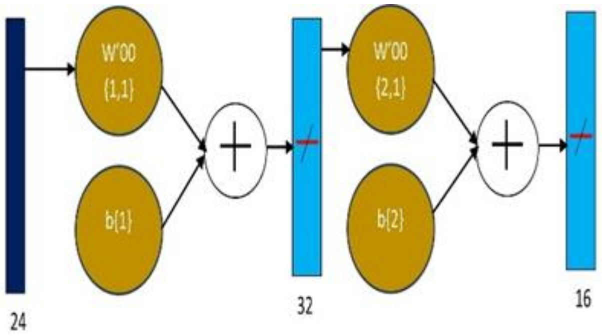

Figure 1 IMCFFNN with Encryption and Decryption Process

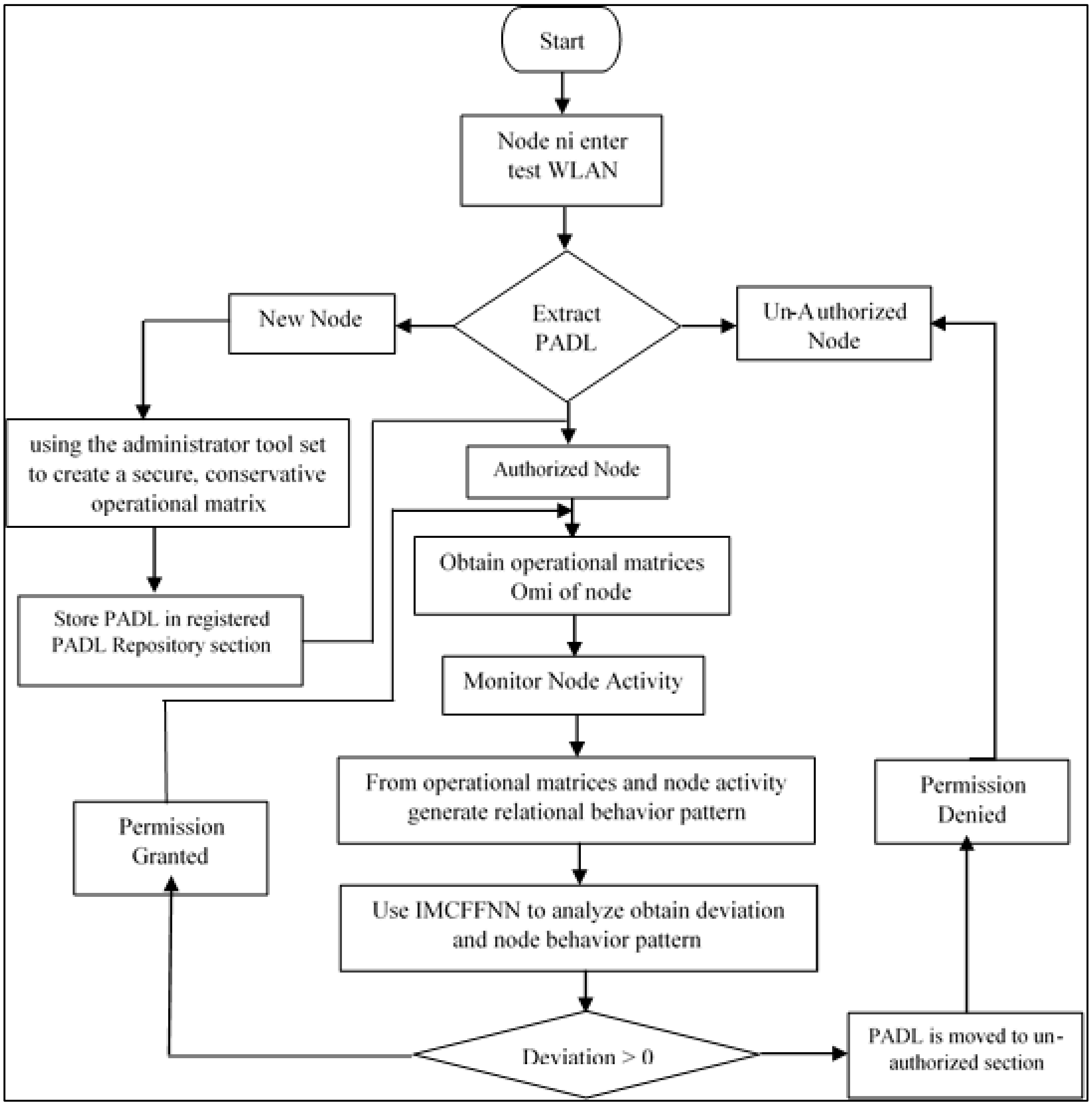
Start
Node ni enter test WLAN
Extract PADL
New Node
Un-Authorized Node
using the administrator tool set to create a secure, conservative operational matrix
Authorized Node
Obtain operational matrices Omi of node
Store PADL in registered PADL Repository section
Monitor Node Activity
From operational matrices and node activity generate relational behavior pattern
Permission Denied
Permission Granted
Use IMCFFNN to analyze obtain deviation and node behavior pattern
Deviation > 0
PADL is moved to un-authorized section

Figure 2 Proposed Architecture

Output layer and classification: In the outer layer, there are just two neurons: Attack and Benign. Since 1024 neurons from the previous layer have to be reduced to only two, a sigmoid activation function has been selected. This article favors the binary classification that had been planned given the sigmoid function's nature, which only produces two outputs. The CSM is thought to form the core of the proposal for a CFA. The CSM is designed to achieve CNs by using neural networks through the implementation of computational programming. Figure 1 gives an overview of the proposed WLAN for CFAs. It requires the use of a CP and an efficient automatic control mechanism, which are considered to be crucial components for CSM design work carried out. As seen in Figure 3, the CSM is giving the wireless network information. It keeps monitoring functions on and records WLAN access.

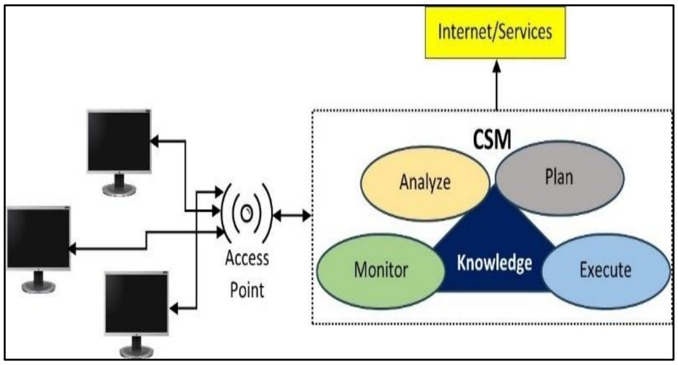

Figure 3 Conceptual CFA

The CFA block diagram is displayed in Figure 4. To accomplish integrity and security in CN, the AC is essential.

It is discovered that CN is vulnerable to node misbehavior, assaults, and jamming. To address all of these issues, networks must offer strong authentication. This needs to be done from a deeper perspective in terms of understanding user node identification and behavior. The above-mentioned problems are addressed by a well-designed CSM, as has already been mentioned.

The CSM has a strong AC approach for the CSM, in addition to its knowledge of network architecture, and is equipped with robust user verification schemes and approaches. The CSM uses a PADL to identify the terminals. The PADL would have been distinct in respect of a specific terminal. It makes CSM's detection of Node abuses, unauthorized access, blocking, etc. a lot easier.

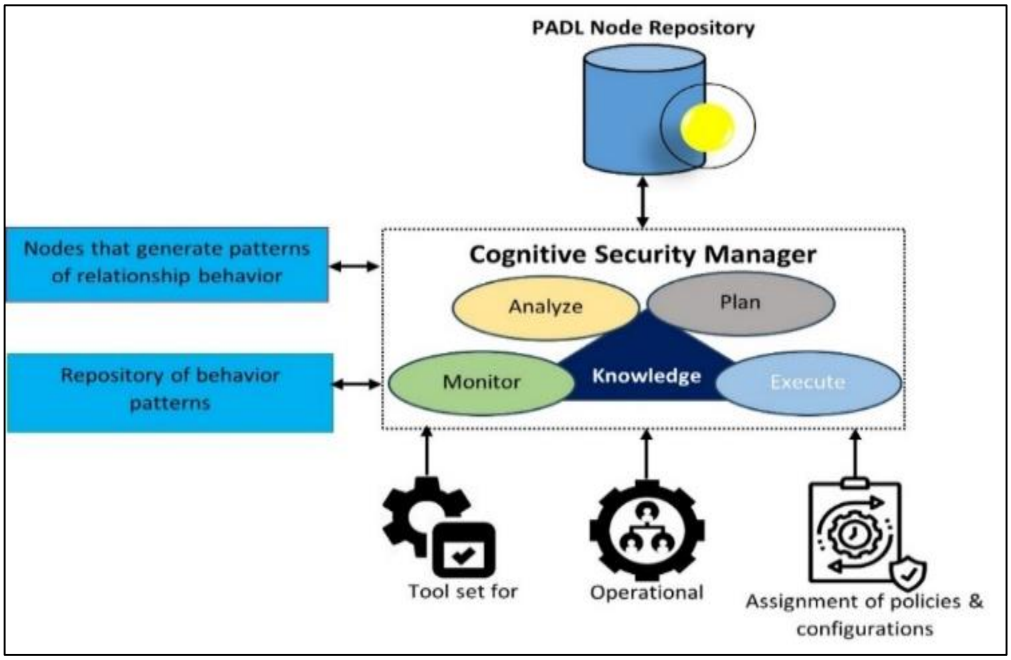
PADL Node Repository
Cognitive Security Manager
Analyze
Plan
Knowledge
Monitor
Execute
Nodes that generate patterns of relationship behavior
Repository of behavior patterns
Tool set for
Operational
Assignment of policies & configurations

Figure 4 CFA Block Diagram

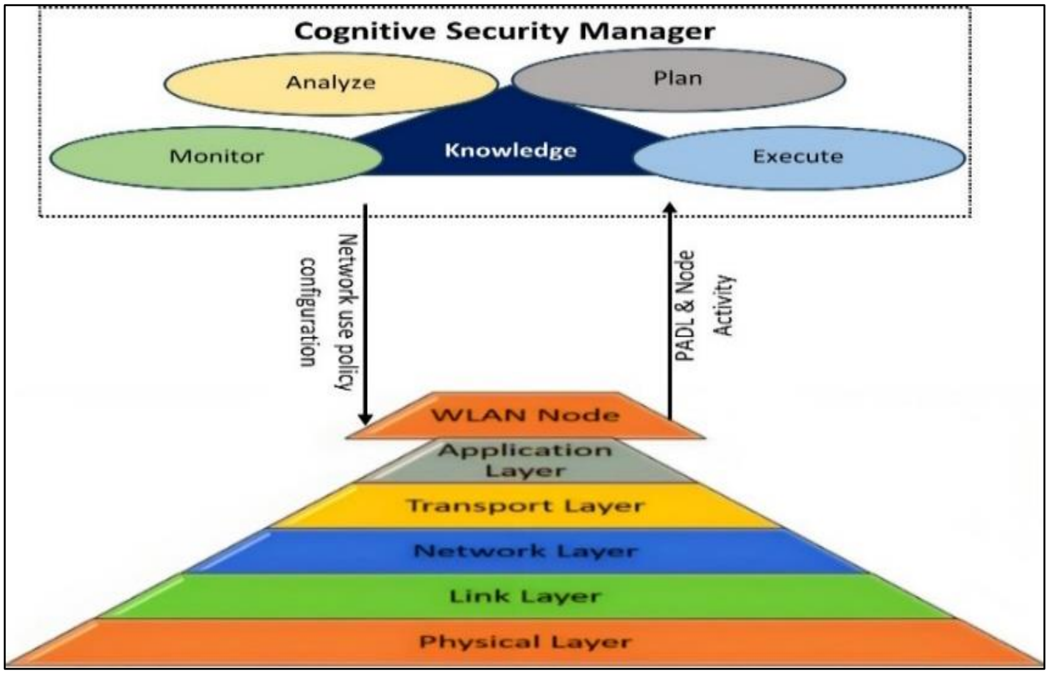

Figure 5 Design of Cognitive Security Manager over WLAN

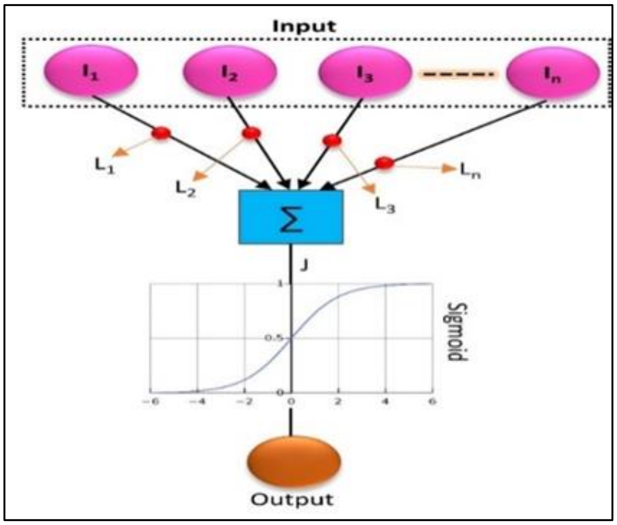

Figure 6 Neural Network Structure on WLAN

It provides a safe and controlled environment for network communications from nodes while preserving information about the constituent parts of the network. The CSM maintains a structured PADL repository, containing both approved and unauthorized sections.

The misbehavior and threats to the network's integrity shall be identified by the CSM PM. Once the terminal has been identified, a PADL repository for the node will be moved from the restricted area to the unauthorized one in the wireless network. CSM shall communicate with the administrative tools set to find nodes inside PADL's permitted and unallowable areas. CSM will initialize a new registered node on its operating matrix according to either the authorized or unauthorized status of that node.

The way CSM is configured and operated can be changed at any time by the network administrator if he or she creates an appropriate tool. This is shown by the adaptive design in Figure 5, which enables CSM to create its existing behavior pattern using an interconnected neural network and then provides for a Relational Behavior Pattern Generator with relevant activity data so that it can perform such behavior patterns as seen in Figure 6.

The production of usage patterns is based upon the relative consumption forecast in a graphic style, making it easier and faster to process. As input, the neural network is able to take into account existing usage patternsi$_t$. The weights of neurons are determined by the user node's administrative network resource or service credentials assigned to it. To further enhance the smoothing of the neural network's output vector, which is represented by Equation (1), Equation (2) uses sigmoid activation.

$$J = \sum_{t=0}^{y} i_t L_t \quad (1)$$

J: NN output

i$_t$: CSM provided input vector

Y: No. of hidden layers

L$_t$: Repository weights

$$Output = \frac{1}{1+e^{-j}} \quad (2)$$

The CSM will be presented with the observed behavior pattern of the node under investigation for analysis.

3.1. Methodology: Description

The proposed algorithm has been implemented in NS-2 (Network Simulator Version 2.0) tool. It is applied to simulate both the networking and routing protocols in wire and wireless networks. It replicates the behavior of the real network. It is an efficient tool which gives accurate result and secured communication. This network consists of 3 nodes (n0-n2). The link existence (duplex in nature) between the nodes is ranges from n0-n1 and n1-n2. The link n0-n1 has 10kbps of band width and 100ms of delay. The link n1-n2 has 5mbps of bandwidth and 200ms of delay. Noe “n0” is having some data to send to node “n2” through noe “n1”, which is a hub device. Each node uses Drop Tail queue of which the maximum size is 10. The TCL language is used to observe the packet flow for the given network in network animator (NAM). The proposed methodology is comprised with the following steps:

3.2. CSM With IMCFFNN

The training set is shown on the network at regular intervals, and weights are adjusted until an overall error has been reduced to a predetermined level. Training could be hampered by local minima because the Delta rule is pursuing a path of greatest good on an error surface. This is partially offset by the term of momentum.

Step 1: The components of input vector is transferred from the input layer to every intermediate layer node

Step 2: Middle hidden layers receive input and compute the outputs

Step 3: The computed output is managed by CSM and send to the output layer for each input vector.

Step 4: if the IMCFFNN not reached the target value then all the hidden layers weight will be updated by using Equation (7)

Step 5: the output layers weight will be updated by using Equation (6)

Step 6: In order to enhance network performance, use Delta rule. Change the weight values accordingly.

Step 7: Compute the error values at both hidden and output layers

Step 8: Calculate the total error if testing network efficiency using Equation (5)

Step 9: From step 2 to step 8 repeat until it reaches the target value.

Step 10: The repetition should not be more than no, of layers in IMCFFNN.

Algorithm 1 CSM with IMCFFNN

The CSM uses an IMCFFNN (Algorithm 1) to analyse the usage patterns of a node so that it can identify adaptive nodes in the wireless network. To develop strong learning and analytical skills, as indicated in Figure 6 the IMCFFNN is used for the assessment of this node's behavioral pattern.

The input, output, and hidden layers are taken into account at three levels of the multilayered feed-forward neural network. The data shall be presented from the left to the right. I_A represents an input vector provided by the CSM. L_{BA} represents the weight connecting unseen neuron B to input elements A, and L_{CB}reflects the weight that connects invisible neuron B to outputs of neuron C. Before calculating their output, every neuron will determine the amount of incentive they receive as input. The weighted sum of inputs and outputs of neurons is used to calculate the net output of neurons based on the activation function or sigmoidal function as specified in the Equation (3), Equation (4).

Where $\mathrm{net}_B^h -$ Output of Bth hidden layer; j_B - hidden layer output

$$\mathrm{net}_B^h = \sum_{N=1}^{N+1} L_{BA} I_A \,\&\, j_B = f\left(\mathrm{net}_B^h\right) \qquad (3)$$

Cth output layer is represented as

$$\mathrm{net}_C^o = \sum_{B=1}^{B=1} L_{CB} J_B \,\&\, Z_C = f(\mathrm{net}_C^o) \qquad (4)$$

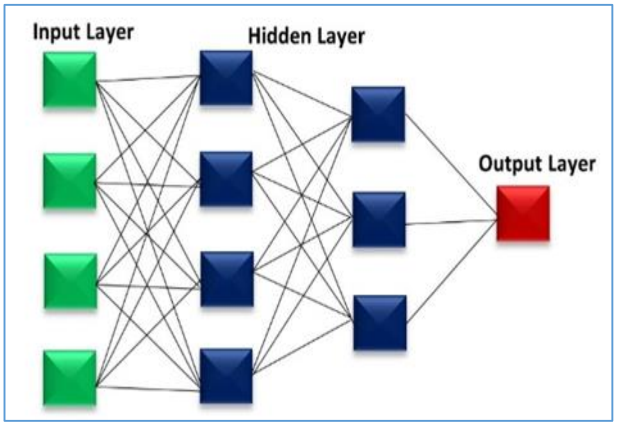

Figure 7 Improved Multilayer CFA Feed Forward Neural Network Architecture

The total error of the network is calculated based on the equation (5).

$$\text{Total Error} = {}^{1}\!/_{2} \left(\sum_{C=1}^{C} (d_C - Z_C)^2\right) \qquad (5)$$

Where d_C is estimated output, Z_C is the obtained output. Output layer error as shown in Equation (6) and the error at hidden layer can be measured as shown in Equation (7)

$$\delta_C = Z_C(1 - Z_C)(d_C - Z_C) \qquad (6)$$

$$\delta_B = J_B(1 - J_B) \sum_{C=1}^{M} V\, \delta_C \qquad (7)$$

Output and hidden layer weight adjustments are represented as $\eta \delta_C J_B$

Output and input layer weight adjustments are represented as $\eta \delta_B I_A$

The CP shall receive information from IMCFFNN, located in the CSM's policy and configuration assignment block. IMCFFNN change the status of a node to an unauthorized one if it finds evidence of infringements, could detect any irregularities or unauthorized access to network services that may compromise network security. Figure 7 illustrates the Improved Multilayer CFA Feed Forward Neural Network Architecture. The data carried over public infrastructure should not be accessible to unauthorized users. The basic idea of encryption is that the data must be mapped with a domain to prevent eavesdropping. The two major types of encryption algorithms are symmetrical and asymmetric. All participants of the symmetric encryption process use a common key. Access to data stored on public infrastructure for unlawful use should not be possible. Encryption is based on the idea that data should be mapped to the domain in a way that prevents eavesdropping. The two most common types of encryption algorithms are synchronous and asymmetric. All parties involved in the asymmetric encryption process use a common key. The encryption and decryption are computed using the equation (8) and (9).

$$E = \text{Encrypt}(K, M) \qquad (8)$$

After the communication across the network, an assigned codeword is received by the recipient and can then be decoded using a common key, i.e.

$$M = \text{Decrypt}(K, E) \qquad (9)$$

Two keys are assigned to each member of an asymmetric encryption scheme: a public key that the user shares with other members and a private key that is only known to them. The encryption function should be theoretical so that a message encoded with the Public Key can't be decrypted where there is no equivalent Private Key, nor will it be decrypted without an identical Private Key. These two keys can be used to provide a logical basis for the relationship between encryption and decryption. If the message is M, Pu_k displays a user's public key for heh users, and Pr_k represents his private key:

$$M = \text{Decry}[Pu\_k, \text{Encry}(Pr\_k, M)]$$

$$\text{if} <Pu\_k, Pr\_k> \varepsilon \text{ Userx}$$

Also:

$$M=\text{Decry}[Pr\_k, \text{Encry}(Pu\_k, M)]$$

$$\text{if } <Pu\_k, Prv\_Ux> \varepsilon \text{ Userx}$$

To send a private communication, the sender therefore relies upon the recipient's public key to encrypt the message before it is sent via Public Infrastructure. In contrast, to unscramble the message that has been encoded, the recipient must use his private key. Another use of an encryption technique is to authenticate a communication's sender. The recipient is aware of the identity of the sender because he or she will only have a key required to complete encryption. To prevent copies from being duplicated and forwarded again, the time and date of creating an encrypted communication could be indicated in the original message. It should be noted that to ensure the confidentiality and authenticity of a message, two levels of encryption can be used. A private key will be used by the sender to encrypt this message and sign it.

4. RESULTS AND DISCUSSIONS

The CSM tracks these network transactions and, to capture a node's behavior through its network activity, it creates usage patterns. To generate the usage patterns, a basic multilayer neural network is used. The activation of the Sigmoid function is part of the ongoing study. To develop effective patterns of behavior, it is necessary to reduce the rate of learning errors in the neural network. Table 1 and Figure 8 and Figure 9 shows the findings of the impact of different neuronal input layer counts.

Table 1 Comparison of No. of Neurons in Input Layer Based on Error % and Response Time

No. of Neurons in I/P layer	Error %	Response Time
10	3.859	1.50483
20	2.895	1.56875
30	3.154	1.53459
40	3.183	1.59677
50	3.098	1.62425

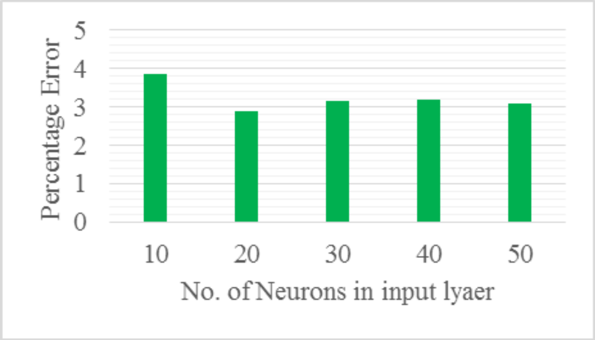

Figure 8 Percentage of Error

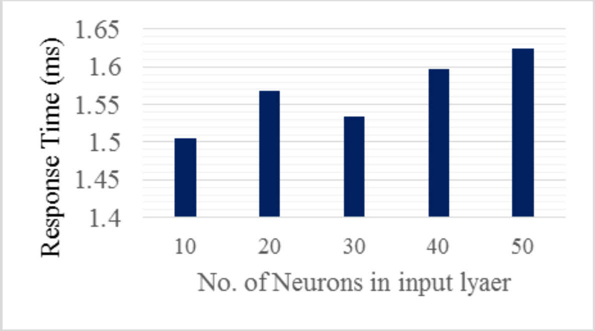

Figure 9 Response Time

The data from observation and analysis show that the rate of error learning is lowest in an input layer network with 20 neurons. There is also a slow response time in the neuron network. Since it is necessary to establish the learning rate of the wireless network, an evaluation was performed on 20 input neurons with different learning rates are shown in Table 2 and Figures 10 and 11.

In the case of a neural network tested, Figures 10 and 11 verify that 0.1 is an appropriate learning rate. The input layer of the neural network contains 20 neurons, which create a user behavior pattern. The results of the neural network testing with learning rates from 0.1 to 0.2 are presented in Tables 3 and 4. Figures 12 and 13 provide a graphic representation of the results.

Table 2 Analysis of Learning Rate, Error % and Response Time

(ŋ) Learning Rate	Error %	Response Time
0.1	2.953	1.3725
0.2	3.237	1.4267
0.3	3.389	1.3964

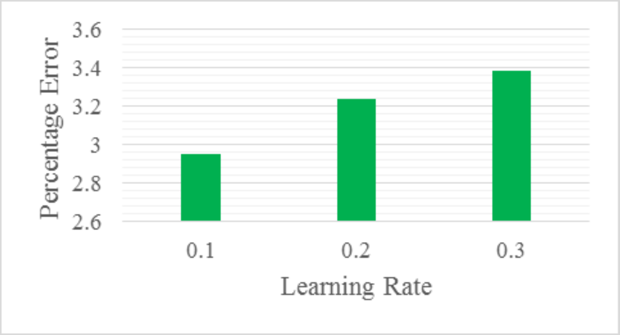

Figure 10 Error %

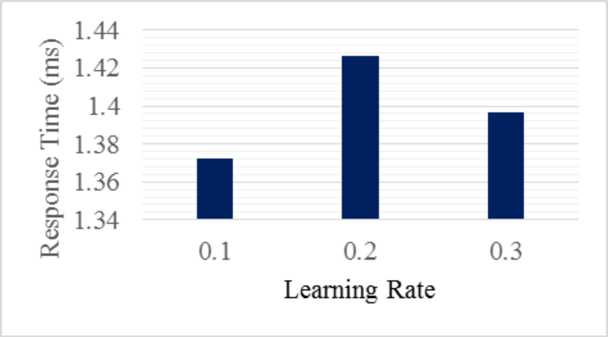

Figure 11 Response Time

Table 3 (Learning Rate (ŋ) = 0.1) Number of Iterations, Learning Error in Percentage and Execution Time

ŋ = 0.1		
Iterations count	Error %	Response Time
1000	3.125	1.9246
5000	3.154	8.4627
10000	1.193	16.8614
15000	1.82	25.9657
20000	1.205	33.6980

Table 4 (Learning Rate (ŋ) = 0.2) Number of Iterations, Learning Error in Percentage and Execution Time

ŋ = 0.2		
Iterations count	Error %	Response Time
1000	3.364	1.9354
5000	1.325	8.9968
10000	1.287	17.3647
15000	1.226	25.5632
20000	1.239	33.6284

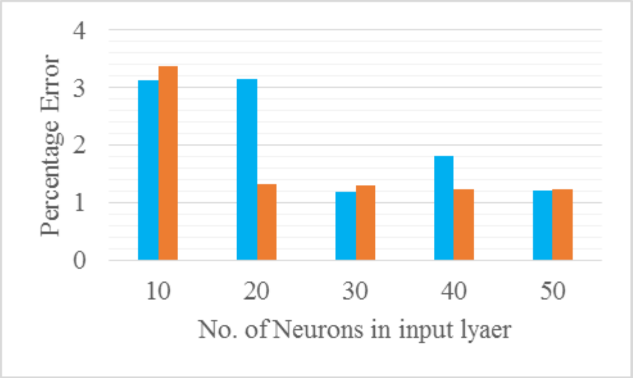

Figure 12 Error %

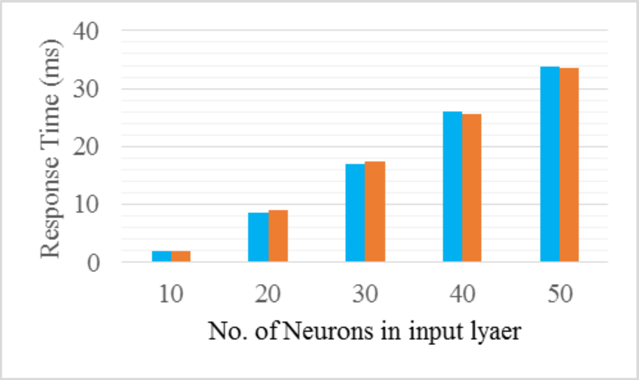

Figure 13 Response Time

The services provided by CSM were unique in terms of consumption behavior in the test bed. Based on the current use of the wireless network, a relational usage pattern has been developed, which is being further explored for the cognitive use CSM with IMCFFNN. Following training, the reply time was observed at 13.649 ms. The CFA is responding swiftly and has no significant impact on network performance. To establish a False Negative Detection (FND) rate and malicious node behavior detection rates, uses neural analyses to detect whether user movements deviate from their real behaviour. The effectiveness of CSM with IMCFFNN method on several other parameters should also be examined in wireless sensor networks. Training tests are being conducted to assess and analyze the quantities of usage patterns that are needed for effective identification; findings have been listed in Table 5. It is further determined to employ 30 usage patterns for effective CSM with IMCFFNN training based on these data. The obtained findings are displayed in Figure 14.

Table 5 CSM with IMCFFNN Training Data Per Node and the FND Rate

No. of training data per node	FND rate
10	13.2476
20	2.06873
30	0.53647
40	0.457
50	0.35691

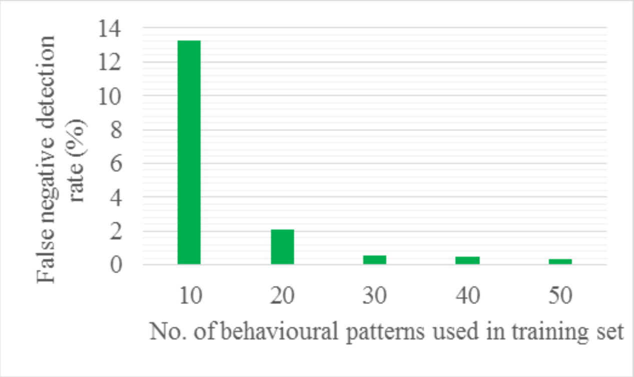

Figure 14 FND Rate

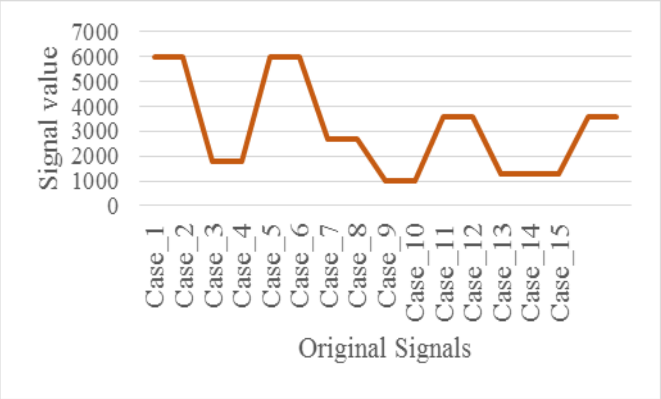

Figure 15 Original Signal Before Encryption

Linear activation parameters have been used for output and hidden layers. If the difference between computed and intended outputs is less than the threshold value, an iteration will be terminated after several iterations.

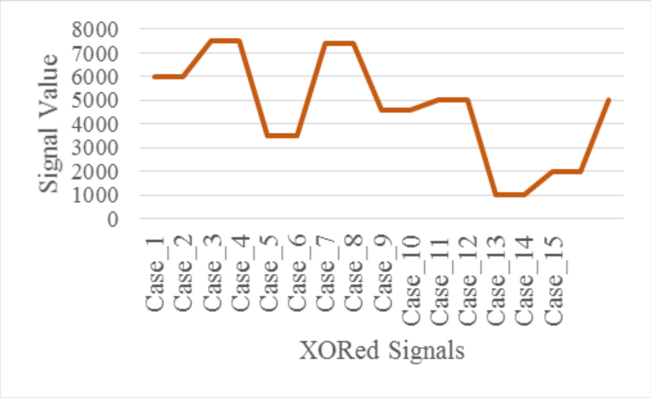

Figure 16 XORed Signals

Figure 15 shows the original signal in its entirety. Figure 16 shows the signal in a bound form. Each time sample's value for this signal is the result of XORed the original signal value from the previous time sample with the encrypted signal value from the current time sample.

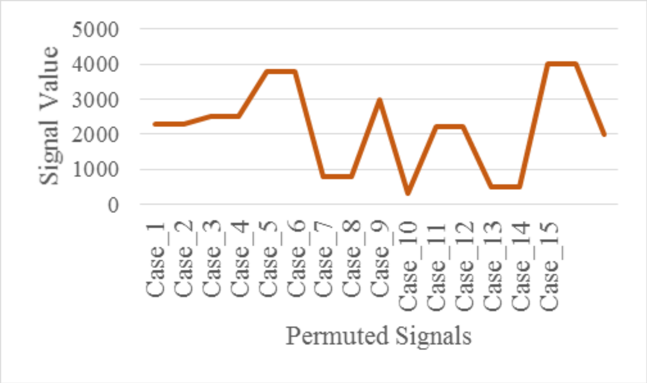

Figure 17 Permuted Signal

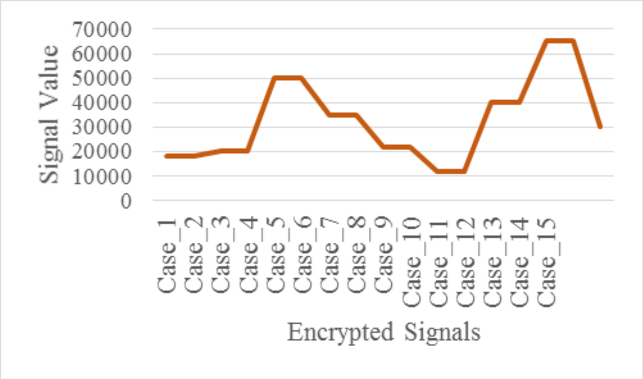

Figure 18 Encrypted Signal

A window is placed over the top 12 bits for our test, and IV's set to "1010101100".

Figures 17 and 18 are illustrative of the permutation and doped signals. The result shows that the encryption method does not provide a context-free operation.

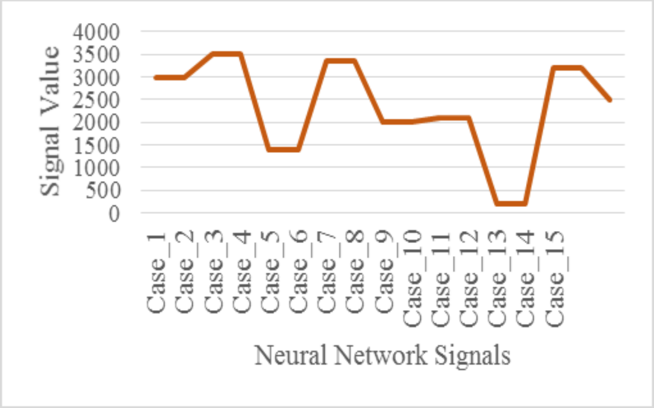

Figure 19 CSM with IMCFFNN Output

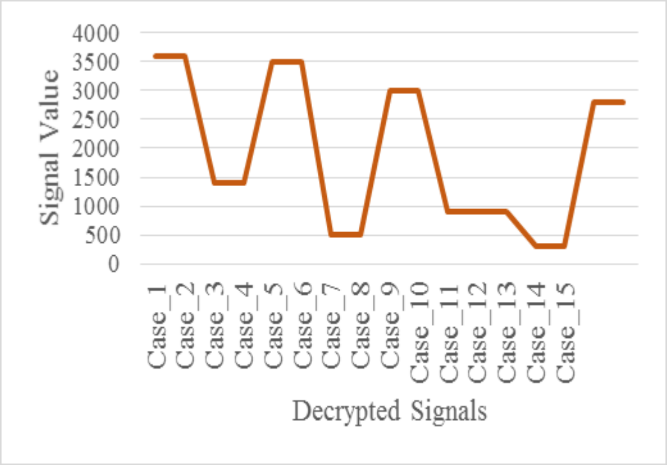

Figure 20 Decrypted Signal

The decrypted signal, although unchanged in the 7th and 8th-time frames, can be noted that its values are distinctly different from one sample to another. The same situation can be observed for time samples 11 and 12. Similarly, Figures 19 and 20 show decryption signals and outputs from an artificial neural network.

5. CONCLUSION

As computer networks expand, the methods of encryption are becoming more and more important. Asymmetric encryption methods have long since been taken into account in particular due to their wide use. However, it has never been simple to find two pairs of functions for encryption and decryption which satisfy the requirements of both functional strengths as well as security. Wireless 802.11 deployment offers high mobility characteristics with simple access to the network thanks to its exponential growth. Since WLANs are unprotected and open to attack, they damage network resource integrity. Advanced security features such as CNs that can measure network dynamics and adjust them are also needed because of the differing characteristics of these wireless networks. With the help of efficient Cognition Engines and AC Mechanisms, the previous design provides sufficient security. To find suitable algorithms for the CN approach, security questions relating to wireless IEEE802.11 networks and constraints on safety measures related to Wi LAN deployment are examined using a literature review. An example is presented of the proposed CFA, which is based on the PADL paradigm and presents intelligence derived from neural networks and AC. The activity was observed on the user node. For training neural networks with monitored past transactions, the backpropagation algorithm is useful. It was observed that user nodes may be classified according to authorized, unknown, and new categories by the PADL-based AC mechanism; furthermore, a complete identification of user nodes can be achieved. Recent observations suggest that the training time of the neural network has increased due to a higher number of user node transactions, which affects monitoring responsiveness. In order to address the deficiencies identified in the previous proposal, CFA architecture has been improved. We present a novel algorithm CSM with IMCFFNN based on artificial neural networks for asymmetric encryption in this study. For the encryption method, we have also put in place a Boolean algebra base model. After that, we've been using the neural network to create a decryption method. The results of the simulations demonstrated, ultimately on networks can be effectively used for decryption once they have been trained.

The CSM with IMCFFNN method achieved approximately 94% detection rates, in comparison with the architecture described above which a detection rate of about 99%.

REFERENCES

[1] Salmi, S., &Oughdir, L. (2023). Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. Journal of Big Data, 10(1), 1-25.

[2] Singh, A., Amutha, J., Nagar, J., & Sharma, S. (2023). A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks. Expert Systems with Applications, 211, 118588.

[3] Fan, F., Chu, S. C., Pan, J. S., Lin, C., & Zhao, H. (2023). An optimized machine learning technology scheme and its application in fault detection in wireless sensor networks. Journal of Applied Statistics, 50(3), 592-609.

[4] Sharma, H. S., Singh, M. M., & Sarkar, A. (2023, January). Machine Learning-Based DoS Attack Detection Techniques in Wireless Sensor Network: A Review. In Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021, Volume 2 (pp. 583-591). Singapore: Springer Nature Singapore.

[5] Srivastava, A., & Bharti, M. R. (2023). Hybrid Machine Learning Model for Anomaly Detection in Unlabelled Data of Wireless Sensor Networks. Wireless Personal Communications, 129(4), 2693-2710.

[6] Gite, P., Shrivastava, A., Krishna, K. M., Kusumadevi, G. H., Dilip, R., & Potdar, R. M. (2023). Under water motion tracking and monitoring using wireless sensor network and Machine learning. Materials Today: Proceedings, 80, 3511-3516.

[7] Abdullah, O. A., Al-Hraishawi, H., &Chatzinotas, S. (2023, March). Deep Learning-Based Device-Free Localization in Wireless Sensor Networks. In 2023 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE.

[8] Ghazal, T. M., Hasan, M. K., Alzoubi, H. M., Alshurideh, M., Ahmad, M., & Akbar, S. S. (2023). Internet of Things Connected Wireless Sensor Networks for Smart Cities. In The Effect of Information Technology on Business and Marketing Intelligence Systems (pp. 1953-1968). Cham: Springer International Publishing.

[9] Gupta, D., Sundaram, S., Rodrigues, J. J., & Khanna, A. (2023). An improved fault detection crow search algorithm for wireless sensor network. International Journal of Communication Systems, 36(12), e4136.

[10] Gola, K. K., Dhingra, M., Gupta, B., & Rathore, R. (2023). An empirical study on underwater acoustic sensor networks based on localization and routing approaches. Advances in Engineering Software, 175, 103319.

[11] Andronie, M., Lăzăroiu, G., Iatagan, M., Hurloiu, I., Ștefănescu, R., Dijmărescu, A., &Dijmărescu, I. (2023). Big Data Management Algorithms, Deep Learning-Based Object Detection Technologies, and Geospatial Simulation and Sensor Fusion Tools in the Internet of Robotic Things. ISPRS International Journal of Geo-Information, 12(2), 35.

[12] Kori, G. S., &Kakkasageri, M. S. (2023). Classification and regression tree (cart) based resource allocation scheme for wireless sensor networks. Computer Communications, 197, 242-254.

[13] Khan, S., &Mailewa, A. B. (2023). Discover botnets in IoT sensor networks: A lightweight deep learning framework with hybrid self-organizing maps. Microprocessors and Microsystems, 97, 104753.

[14] Fredj, N., Hadj Kacem, Y., Khriji, S., Kanoun, O., Hamdi, S., & Abid, M. (2023). AI-based model driven approach for adaptive wireless sensor networks design. International Journal of Information Technology, 15(4), 1871-1883.

[15] Subramani, S., & Selvi, M. (2023). Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks. Optik, 273, 170419.

[16] Oliveira, L. L. D., Eisenkraemer, G. H., Carara, E. A., Martins, J. B., & Monteiro, J. (2023). Mobile localization techniques for wireless sensor networks: Survey and recommendations. ACM Transactions on Sensor Networks, 19(2), 1-39.

[17] Jain, K., Kumar, A., & Singh, A. (2023). Data transmission reduction techniques for improving network lifetime in wireless sensor networks: An up- to- date survey from 2017 to 2022. Transactions on Emerging Telecommunications Technologies, 34(1), e4674.

[18] Pawar, M. V. (2023). Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. International Journal of Pervasive Computing and Communications, 19(1), 124-153.

[19] Ezhilarasi, M., Gnanaprasanambikai, L., Kousalya, A., & Shanmugapriya, M. (2023). A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. Soft Computing, 27(7), 4157-4168.

[20] Rabhi, S., Abbes, T., & Zarai, F. (2023). IoT routing attacks detection using machine learning algorithms. Wireless Personal Communications, 128(3), 1839-1857.

[21] Yadav, P., & Sharma, S. C. (2023). A systematic review of localization in WSN: Machine learning and optimization- based approaches. International Journal of Communication Systems, 36(4), e5397.

[22] DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). A survey of AI-based anomaly detection in IoT and sensor networks. Sensors, 23(3), 1352.

[23] Mall, P. K., & Singh, P. K. (2023). Credence-Net: a semi-supervised deep learning approach for medical images. International Journal of Nanotechnology, 20(5-10), 897-914.

[24] Subramani, S., & Selvi, M. (2023). Intrusion detection system using RBPSO and fuzzy neuro-genetic classification algorithms in wireless sensor networks. International Journal of Information and Computer Security, 20(3-4), 439-461.

[25] Hajializadeh, D. (2023). Deep learning-based indirect bridge damage identification system. Structural health monitoring, 22(2), 897-912.

[26] Seyfollahi, A., Taami, T., & Ghaffari, A. (2023). Towards developing a machine learning-metaheuristic-enhanced energy-sensitive routing framework for the internet of things. Microprocessors and Microsystems, 96, 104747.

[27] Rafique, S., Gul, S., Jan, K., & Khan, G. M. (2023). Optimized real-time parking management framework using deep learning. Expert Systems with Applications, 220, 119686.

[28] Booth, T. M., & Ghosh, S. (2023, April). A Gradient Descent Multi-Algorithm Grid Search Optimization of Deep Learning for Sensor Fusion. In 2023 IEEE International Systems Conference (SysCon) (pp. 1-8). IEEE.

[29] Nagy, M., Lăzăroiu, G., & Valaskova, K. (2023). Machine Intelligence and Autonomous Robotic Technologies in the Corporate Context of SMEs: Deep Learning and Virtual Simulation Algorithms, Cyber-Physical Production Networks, and Industry 4.0-Based Manufacturing Systems. Applied Sciences, 13(3), 1681.

[30] Mohammed, S. K., Singh, S., Mizouni, R., & Otrok, H. (2023). A deep learning framework for target localization in error-prone environment. Internet of Things, 22, 100713.

[31] Alghamdi, R., & Bellaiche, M. (2023). A cascaded federated deep learning-based framework for detecting wormhole attacks in IoT networks. Computers & Security, 125, 103014.

Authors

Dr Senthil Kumar S received his first degree from Madras University, Computer Science, India, in 2005. He has also Master degree from Thiruvalluvar University, Computer Applications, India, in 2008. The Ph.D. degree from the Department of Computer Applications in Manonmaniam Sundaranar University, India in 2019. He is currently serving as an Assistant Professor in Department of Computer Applications at SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India. His main research interests focus on Web Metrics, Web Services, Computer Networks, Image Processing, Data Mining, and Text Mining.

Dr Suganya J is currently working as Assistant professor in the Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, SRM Nagar, Trichy. She has received her doctoral degree from AVVM Sri Pushpa College (Autonomous), Poondi, Thanjavur Dt. affiliated to Bharathidasan University, Tiruchirappalli. She has qualified State Eligibility Test (SET) in Computer Science from Mother Terasa University, Kodaikanal. She has 14 years of teaching experience. She has published two Patents and research papers in various National, International Journals and authored one book. Also, she acted as a resource person in seminars and workshops. She received two awards for academic excellence. She is acting as editorial member in peer reviewed journals.

RESEARCH ARTICLE

Dr Kanagalakshmi K is working as an Associate Professor in the Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology (Deemed to be University), Trichy, Tamilnadu, India. She has 23 years of teaching experience the collegiate education. She has published more than 34 research papers in International Journals of repute and presented more than 75 papers in International, National and State level Seminars, Conferences together. She has produced M.Phil. and Ph.D. Scholars. She has published 5 books and 3 Patents. She has received 8 awards like Best Faculty Award, Best Scientist Award, Best Principal Award etc. Her areas of interest include Biometric, Pattern Recognition, Digital Image Processing, Security etc.

Dr Hariharan C is working as an Assistant Professor in the College of Management Studies, Faculty of Science and Humanities, SRM Institute of Science and Technology (Deemed to be University), Trichy, Tamilnadu, India. He obtained his M.B.A with Specialization in Finance and Human resource from Nehru Institute of Information Technology & Management, Coimbatore. He completed his Bachelor degree (BBA) in Thiru. Ve. Ka Government Arts College and He awarded Doctorate degree from Bharathidasan University. His research concentrated on Exploring Investors quality towards formal and sustainable investment: A differentiation analysis of rural and urban investors. He has published More than 40 articles in reputed peer-reviewed National and International Journals, 5 chapters. He has organized ICSSR Sponsored two days International Seminar on MSMEs & Covid 19. He has strong interest in doing Statistical Analysis. He has made significant contributions to research in the field of Financial Services and Markets, Behavioral Finance, Sustainable Investments.

How to cite this article:

Senthil Kumar S, Suganya J, Kanagalakshmi K, Hariharan C, “Development of Hybrid Cognitive Security Managers on Improved Multilayer CFA Feed Forward Neural Network to Improve the Security on Wireless Networks”, International Journal of Computer Networks and Applications (IJCNA), 11(3), PP: 290-303, 2024, DOI: 10.22247/ijcna/2024/18.