6. CONCLUSION AND FUTURE WORK

6.1. CONCLUSION

Wireless 802.11 deployments provide rich mobility features with ease in network access owing to their tremendous growth. The WLANs are insecure and vulnerable to attacks, affecting the network and its resource integrity. These diverse WLANs require advanced security mechanisms like CNs capable of understanding the network dynamics and adapt accordingly.

The research work undertaken here has been carried out extensively to design and develop CFAs to provide security to the existing IEEE802.11 network. The work is supported by detailed literature survey in this area. The satisfactory security aspects are achieved through the above architecture by integrating AC Mechanisms and effective Cognition Engines. With the support of the mentioned literatures, the security problems associated with wireless IEEE802.11 networks and drawbacks of the security mechanisms in WLANs deployments are discussed to arrive at the relevant algorithms for CN Approaches. The soft computing approaches adopted to achieve cognition and highlights on Neural Networks trained using Back Propagation Algorithm, MFNN and Kohnen SOM have been proposed.
The Proposed CFA, where AC using PADL concept and intelligence imparted using neural networks is presented. The user node behavior was monitored. Monitored previous transactions are helpful to train the neural network through the Back Propagation Algorithm. It has been observed that the PADL based AC Mechanism is able to achieve complete User Node Identification and able to classify the user nodes into authorized, unauthorized and new nodes. The behavior of user nodes monitored based on their network transactions are analyzed using the back propagation neural networks. Increase in the user node transaction has led to higher training times for the neural network effecting responsiveness in monitoring.

To overcome the drawbacks of the previous architecture the CFA Architecture has been enhanced which incorporated similar AC Mechanisms based on the PADL of the User Nodes where the difference is shown to be that the numerous user transactions have been used to generate usage patterns. These patterns are being analyzed using Multi-Layer Feed Forward Neural Networks to achieve cognition. This supervised learning technique is compared with unsupervised learning techniques for identification of malicious nodes. The SOM based technique achieved a detection rate of about 94% compared to the presented architecture which achieved about 99% detection rates.
The work undertaken here has contributed to the security aspects of wireless local area network as per the results analyzed and presented.

6.2. FUTURE WORK

The research presented here lays a strong foundation for implementation and realization of CNs. It can also apply to various other networks like Wireless Sensor Networks, Ad-Hoc Networks, Cloud Computing and many more. The cognition engine developed mainly relies on the intelligence provided by the neural networks.

To achieve cognition, designing neural network configuration plays a major role. The usage of Dynamic Neural Network or similar techniques could be considered for future research in achieving cognition. CNs are relatively immature, additional work has to be done to provide complete solutions for its acceptance.