Journal of Information Technology and Cyber Security Engineering
Volume 01, Issue 01, July 2025
www.ijitcse.com

Hopfield Neural Network-Based Rogue Access Point in a Wireless Area Network

K Kaveri[1] and M Sangeeta[2]
Department of Computer Science Engineering, Hindustan University, Chennai
[1]Corresponding Author: kavericse2233@gmail.com

To Cite this Article
Kaveri and Sangeeta, "Hopfield Neural Network-Based Rogue Access Point in a Wireless Area Network", Journal of Information Technology and Cyber Security Engineering", Vol. 01, Issue 01, July 2025, pp:20-23.

***Abstract**: The idea presented here is a technique to spot rogue access points (RAPs) in wireless area network (WAN) using Hopfield Neural Networks (HNNs). RAPs offer severe security threats since they simulate real access points to capture user data or launch attacks. Evolution of the proposed model. The proposed model has the capacity to detect faults in network behavior such as MAC address spoofing, unusual signal strength, and traffic patterns with the help of the associative memory and pattern recognition properties of Hopfield Networks. The technology can identify the aberration that is indicative of the rogue devices through the training of the network using genuine access point parameters. The HNN-based scheme is a potential alternative to real-time monitoring of wireless networks that might be used in the security of the networks because simulation results indicate that the level of detection accuracy, false positive errors, and rapid response times are tremendous.*

***Keywords**: WLAN, rogue access point, neural network, Hopfield algorithm, and wireless communication*

I. Introduction

One of the most important aspects of wireless communications today is security especially at a time when Wireless Area Networks (WANs) have become widespread within the home, work environment and in the open spaces. One of the largest security risks is the presence of Rogue Access Points (RAPs), unauthorized wireless equipment that tries to impersonate legitimate access points so as to mislead users and capture and steal their confidential data. These RAPs present dangers in the form of data steal, unauthorized access and denial-of-services and they can be deliberate on the part of the attackers and non-intentionally on the part of the users. To identify activities of complex or adaptive rogue, the traditional methods of detecting may use human inspection or may utilize static rule-based tools, which is slow and inefficient in detecting. In an attempt to curb this challenge, this paper proposes the implementation of a Hopfield Neural Network (HNN) in detection of RAP. The HNN is a kind of recurrent artificial neural network, ideal on pattern recognition and associative memory tasks. The system can also identify the unusual events, which point to rogue traffic, by learning the network using the known characteristics of genuine access points, including the MAC addresses, intensities of signals, and the network IDs. This is capable of adaptive, real-time identity recognition with a higher accuracy rate and a reduced rate of false positives because of being based on a neural network. In its dynamic environment, the proposed paradigm can be used as a valid approach to enhancing wireless network security.

II. Rogue Access Point

Rogue access points (RAPs) are unauthorized wireless access points installed somewhere inside secure networks, often without any knowledge or authorization of the network administrator. RAPs can either be inadvertently brought by employees on their personal gadgets or deliberately brought by hackers. Such devices pose major security risks as they can be able to bypass authentication measures allowing unauthorized individuals access the network and access sensitive data or introduce malware to the network. RAPs can be of two types; malicious RAPs, which are set to mimic legitimate APs so as to steal users' credentials or intercept traffic, and non-malicious RAPs which are often installed as a convenience but can be malicious as well because they are not usually configured properly or with encryptions. It may be harder to locate RAPs especially due to the crowded wireless condition that attackers may take advantage of the same SSID and masquerade MAC addresses. Effective countermeasures include real-time monitoring, neural network-based anomaly detection so as to detect a suspicious access point activity as well as wireless intrusion detection systems (WIDS).

III. Literature Survey on Rogue Access Point

Several studies have been conducted in the recent years to investigate the methods of detecting and mitigating rogue access points (RAPs) that are an increasingly popular issue in the area of wireless networks security. The common ways include rule-based filtering and signature-based detection which are basically conventional methods in which the characteristic of incoming access points (like MAC address, SSID and frequency) are compared with those of the database of the recognized authentic equipment. These methods however find little success against experienced attackers who use spoofing and the random nature of network configurations. To track down the traffic across a network and also identify unauthorized access points (AP)s, through differences in signal strength and unusual connection patterns, a few researchers have put forward Wireless Intrusion Detection Systems (WIDS). Although such systems are effective, they require constant human update and false positives are quite high. The recent development has focused on machine learning and artificial intelligence-based techniques such as decision trees, support vector machines (SVMs) and neural networks. These models enhance the detection in terms of their accuracy by identifying deviations and knowing normal patterns of network. In particular, Hopfield Neural Networks (HNNs) and deep learning approaches have been shown to prospective in wireless applications, particularly in the anomaly identification and pattern recognition. In order to efficiently detect RAPs, the literature finds it appropriate to stress the importance of context-aware analysis, adaptive algorithms, and monitoring in real-time execution. However, scalability, minimization of false alarms and ensuring a rapid response in high-density network scenarios remain a problem.

IV. Hopfield Neural Network (HNN)

The Hopfield Neural Network (HNN) is a variant of recurrent artificial neural network dedicated to associative memory and pattern recognition application. It consists of a single layer of neurons interconnected to one another, and each neuron is both, an input and an output node. The network can operate in such a mode until its state reaches a stable or energy minimum in an asynchronous or synchronous state update, a binary mode or a continuous mode. HNN particularly excels at recognizing stored patterns and optimisation problems even when noisy or incomplete data are provided. It guides the network through all states of stable equilibrium representing the learnt patterns with the help of a defined energy function. HNN finds extensive use in image processing, defect detection, security because of its ability to recognize patterns and abnormalities.

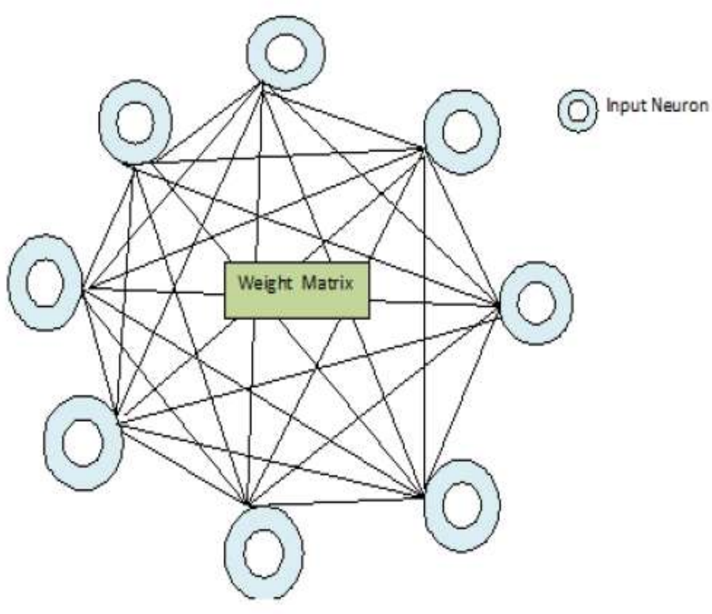

Fig 1: Hopfield neural network

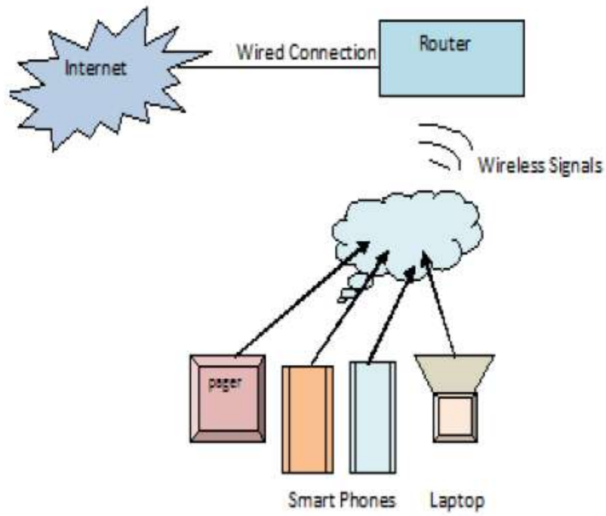

Fig 2: Router connected to devices

V. Simulation Design

One of the simulations of Hopfield Neural Network (HNN) involves developing a model that stores and recalls patterns within an associative memory. The first step is to define the network design, this is typically a full linked network, whereby all the neuron is connected to all other neuron except to itself. The difference between the input pattern complexity and the amount of the neurons are correlated. The weight matrix is configured during training by the outer product rule or Hebbian learning, weights are enabled by the patterns to be memorized. Input is fed into a network at the stage in which the network is recalling. Input injected into the network can be noisy or partial. Then states of the neurons are changed either simultaneously or sequentially, with a predetermined activation function, usually a sign or sigmoid function. The network keeps evolving until it achieves a stable network state (energy minimum), which is one of the stored patterns. The simulation may be done with the use of neural simulation tools, MATLAB, or Python.

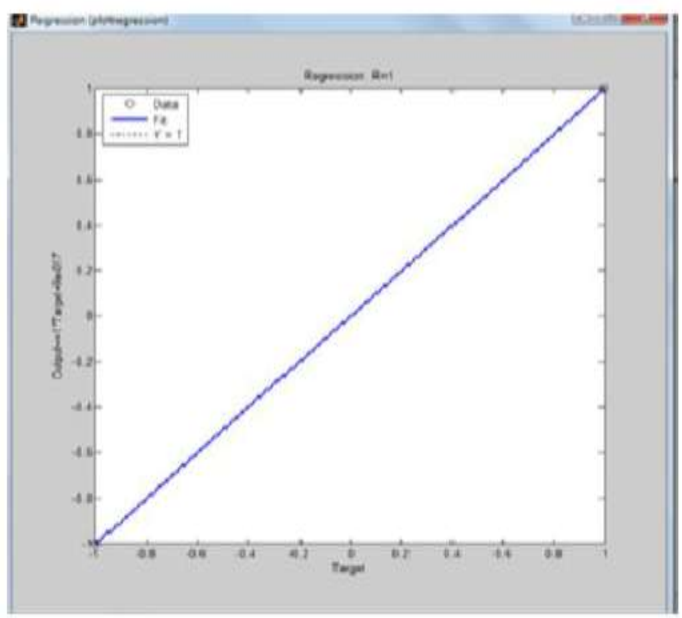

Fig 3: Training graph for Network

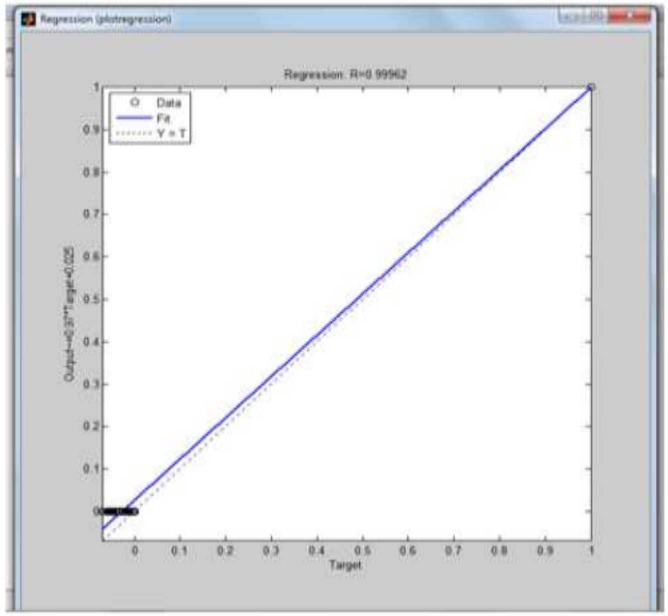

Fig 4: Input and output in graph form

VI. Conclusion

To sum up, the approach based on Hopfield Neural Network (HNN) is an efficient and clever approach to detection of rogue access points (RAPs) in wireless area networks. By consuming the pattern recognition and associative memory features that are offered by HNNs, the system can identify abnormalities in access point behavior with utmost accuracy such as MAC address spoofing, illegal SSID broadcast and inconsistent signals. In comparison to traditional methods, simulation results have demonstrated superior detection (including reduction of false positives), plus rapid response time. Since they are dynamic and flexible, HNNs may operate effectively in a dynamic and complicated wireless ambiance. This paper shall show how neural network security solutions are able to enhance the security of a wireless network and why they can be used in the critical infrastructure, public network and in the enterprise.

References

[1] A. Amruta Singh, Anila Nayar and Shamukh Nayyar, "Wifi and LAN in security breaches in Sodar system" IEEE Trans. Andhra University, vol 1(7), pp 231-248, 2000.

[2] Y Sokamso Tayang, Hubert and Anil Kumar Yadav, "Harmonica and non-harmonics in LAN and WAN in monitoring systems", Springer Lecture notes, NIT Warangal, vol 5(3), pp463-472, 1998.

[3] M Koel Singh, Ravindra nath and Hima Bindu, "*Management of neural networks in WAN and LAN wifi networks", IEEE Trans. PES University, Bangalore, vol 5(2), 2001*.

[4] G. Gopichand and R. K. Saravanaguru, "A Generic Review on effective Intrusion Detection in Ad Hoc Networks," *International Journal of Electrical Engineering (IJEE)*, vol/issue: 9(2), pp. 732-743.

[5] N. Prasad and A. Prasad, "WLAN Systems and Wireless IP for Next Generation Communications," Artech House, Inc. Noorwod, USA, 2002.

[6] "Rogue Access Point Detection‖ Automatically Detect and Manage Wireless Threats to Your Network," www.wavelink.com.