CHAPTER 1

1. INTRODUCTION

1.1 Overview

Life, as we know today has become very hectic and every man is always on the move, so to speak and hence his activities are time scheduled. In recent years a new trend for employees ‘work from home’ has emerged with the great impetus. Also we frequently encounter with the scenario of a person working while commuting. In view of the above factors the need for wireless communication will arise, wherein whose network standards are defined in IEEE 802.11, which directs to afford wireless network communication. Wireless Networking has been growing proportional to the Internet because Wireless Local Area Network (WLAN) offering easy anywhere anytime access to the networks, ever since the Internet users and the concerned are enjoying the user friendliness of the wireless network.

Wireless Networks have many advantages which provide various options of seamless integration of varied communication systems which aids in the smooth functioning of the economy. Security issues are associated with wireless networks in view of the information transmission through air and the consequent risk involvement. The Access Point (AP) being the link between the wired and wireless network. It has been noticed that the current wireless APs which are meant for the
protection of internal resources from external threats, pose considerable security problems [1, 2, 3].

Many organizations based on relevant documents by the supplier says that the security measure in terms of APs are acceptable to avoid unauthorized access and use. Myriad mechanisms for security measures for privacy, validation, and AC (AC) are these being susceptible in nature.

WLANs have experienced a tremendous growth in the past decade, where in they offered easy, anywhere and anytime access to networked resources. Also they offering varied services like internet connectivity etc., generally characterized by its mobility, cost-effectiveness and high data transmission rates. On the other side, wireless networks lack to readily provide sufficient and effective security mechanisms, which is being major feature to provide the security to the WLANs, as per the past history of the WLANs, they face the problem of security and research work is going on in the area to secure the WLANs and to make the network more secured and reliable. Researchers have developed various security mechanisms liked key based security, encryption etc., which have proved to be ineffective in compromising the integrity of the wireless network [3].

Initially WLANs came with the Wired Equivalent Privacy (WEP) security and within short span of time WLANs became more popular but WEP security failed to provide the required security to the network, On
account of many flaws in the same [4, 5, 6]. Innovative techniques have been proposed to find solutions to the problems of WEP. As result of Innovation Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access version 2 (WPA2) came into existence. The researcher also found that, some threats and attacks have been discovered on WPA and WPA2 [19, 22, 28, 36, and 46].

The research work undertaken here, to provide intelligent wireless security architecture to alleviate the deficiencies prevailing in the current wireless network deployments. It has succeeded in providing cognition using soft computing techniques [68]. The proposed architecture achieves security through AC mechanisms and cognition technique. AC mechanism is based on the PADL and Cognition which means self-awareness, self-management and self-healing have been achieved using neural networks and fuzzy rules.

Network evolution for self-awareness, autonomous status and adaptive networking attempts have been done to overwhelmed the inadequacy of organizing and handling wireless networks,

which clues to deprivation of Performance and Quality of Service (QoS). Enhancement of network operations, include Self-consciousness, Self-administration and Self-Healing touch have been projected.

This has produced a new vista in networking termed as the Cognitive Networking, processing perceptive properties, which are learning,
adaptation, and goal optimization. Study and analysis of available research proposals highlighted in the literatures led to the design of desired CN architecture capable of adopting the specific CN techniques. With necessary discussion and analysis based on the essential stuffs of the cross-layer design for CNs and placement issues has been quantified. The security mechanisms are quantified in terms of valid user identification with specific objective.

1.2 Motivation

The current WLANs are vulnerable and pose a huge threat to network integrity. The present access control mechanisms provided in the existing WLANs deployments like WEP, WPA, WPA2, MAC Filtering, Internet Protocol (IP) Based Filtering and a few more could easily be bypassed leaving the WLAN open and unsecured [7, 8, 9, 10]. Many tools have been identified to break the AC mechanisms presently deployed [11, 14, 15, 16, 17].

Secured Networks could be established to provide their AC mechanisms robust. Nodes identified within a network and their behaviors of the Nodes accessing the WLANs have been studied to provide security [72, 74]. Soft Computing techniques have been used to study the behavior of the user nodes [68]. CNs are also known as “Smart Networks” [47] and have the capability to observe the Node Behavior in the Network, to orient the behavior in deriving a usage pattern for
analysis, based on the obtained pattern which decides the composition of the usage pattern. On the basis of the usage composition, subsequent response action has been undertaken.

CNs are realized based on a Cognitive Process (CP). Cognition has been studied and debated by researchers during these days, where in multiple approaches have been suggested to achieve cognition. Cognition Engines impart the intelligence required to understand and observe the behavior of network condition to achieve cognition using estimation, game theory, evolutionary computing, fuzzy logic, and Markov decision models, pricing theory, theory of social science and reinforcement laws [68].

Evolutionary Computing algorithms like Genetic Algorithms have been considered by many researchers to achieve cognition. In this proposed research work the neural networks concepts are used to achieve cognition using Multi-Layer Feed Forward Neural Networks. Back Propagation learning based on neural networks is also proved to be very efficient [74].

User Nodes AC mechanisms like Fast Authentication and Authorization have been used in building CNs and the work presented here is uses PADL in providing AC in the proposed approach. It has been identified that user node behavior analysis and the user node behavior reputation known to be critical in providing cognition. User node behavior has been analyzed by researchers using game theory, fuzzy
logic and many other techniques.

Unsupervised learning techniques like Self Organizing Maps [71] have also been used in the past to incorporate intelligence in the CP. From this undertaken research work, it can safely conclude that to secure a WLANS strong AC Mechanisms and CNs are to co-exist. This paradigm is to define the new approach to secure WLAN.

1.3 Objectives and Scope

The research undertaken is targeted towards providing security to WLANs using cognitive approaches and Access Control (AC) mechanisms. To realize secured intelligent WLANs, the research work undertaken is to develop a framework named as cognitive framework Architecture (CFA), wherein core of the CFA is the Cognitive Security Manager (CSM). CFA is identified to be embedded with both AC mechanisms and cognition engines.

a) AC: AC mechanisms are considered to be basic steps in the construction of secured WLANs. In the proposed research work undertaken is to provide User Identification and AC Mechanisms based on the PADL. The PADL of every Node is unique and obtained using the cross layer definitions of the user nodes. The PADL extracted is used for registration, identification and authentication of user nodes within the cognitive framework.
b) **Cognition Engine**: The CFA is managed by the Cognition Security Manager (CSM) which will integrate the user identification based on PADL to monitor the data transaction ongoing within the WLANs under consideration. The work highlighted has a framework describing Administrative Tool Set, which houses the authorized network transaction, which is being used by the Policy Manager (PM) for network transaction analysis based on neural network approach for transaction analysis.

Also it has been evaluated and refined the CFA to detect user node misbehavior, providing AC and securing the network based on the dynamic changing network scenarios. Experimental Evaluations reported here shows appreciable misbehavior detection rate compared to the existing prevailing techniques and also rapid network response time.

**1.4 Research Contributions**

The research work presented here justifies the cognition process to secure WLANs deployments where in the major contribution of the research is in two areas, which have been given below,
a) AC using PADL

Security could be provided by incorporating robust AC Mechanisms. The entire User Node’s PADL is essential to ascertain the nodes and record them on the network.

User Node filtration on the existing systems only rely on MAC filtering, IP Filtering and Key based security mechanisms which are vulnerable. The experimental results discussed prove the dependability of this AC mechanism, wherein the reliable AC Mechanism provides a much need based security environment where User Nodes misbehavior detected prevents network resource access, thus preventing overhead of additional monitoring required.

b) Cognition achieved by monitoring the user node pattern

The users of WLANs deployments and their usages vary dynamically which is based on the understanding of user node behavior cognition achievement. The CFA discussed incorporates intelligence using MFNN to analyze user transactions wherein the neural network developed proved to be very good observers and analyzers of their user nodes behavior. The Cognition Engine has developed achieved higher malicious user node detection rates of up to 99% on successful training. This high detection rates is being obtained to justify the CFA design providing security to accommodate the dynamics of the IEEE802.11 WLANs.
1.5 Outline of the Thesis

The contents of the portions of the thesis are organized as follows:

Chapter 2 has presented the existing 802.11 architecture, which highlights the discussion about the existing security mechanisms available with 802.11 networks. The drawbacks of the present security mechanisms are clearly identified and the proposed cognitive technique is discussed to overcome the security lapses. Discussion has on the differences between CNs, cognitive radio, and Existing CN architectures and also the use of Soft Computing Techniques to achieve cognition. The importance for AC for Wireless Networks and Cognition Engine Algorithms used by researchers are also discussed in this chapter.

Chapter 3 Discuss on the Soft Computing techniques adopted by the author to achieve cognition based on BPNN, Multilayer feed forward neural networks and Self Organizing Maps are highlighted.

Chapter 4 presents the proposed CN architecture, wherein AC is achieved using PADL and Cognition based on BPNN techniques. The architecture proposed has been thoroughly investigated and the results are provided. The results of the proposed Cognitive Technique are provided in Comparisons with the existing Self Organization Maps cognition engine results.
In the Chapter 5, improved designed architecture with the introduction of User Behavior Pattern and the Behavior analysis achieved by using Multilayer Feed Forward Neural Networks trained using Back Propagation is discussed with evaluations and observations.

Chapter 6 presents the discussion on the future scope and the improvement of present work and also the conclusion of the present research work.