

National Conference on "Research Innovations in ICT and Computing Technologies" (NCRICT-2023)
Special Issue of Journal of Innovation in Sciences (Online), ISSN: 2394-8051

Wireless LAN Network Security using Neural Networks

¹Prof. Sachin Y. Zade, ²Dr. Aruna J. Chamatkar and ³Dr. Pradeep K. Butey
¹Assistant Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur
zade.sachin02@gmail.com

²Associate Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur

³Ex-Head, Department of Computer Science, Kamla Nehru Mahavidyalaya, Nagpur

Abstract: It is life-threatening to keep information secure from unauthorized people and organizations. When a network is compromised, information is taken. In intrusion detection system detects both known and unexpected stabbings that allow a network to be ruptured. The intrusion detecting model detects anomaly and misuse-based attacks. The Wireless Local Area Networks succeeded in delivering wireless network access at low costs. The ANN strategy can be utilized as a part of active way to make the encryption procedure challenging to break and in the interim remarkably trusty. Wired equipment privacy provides security to wireless network by encrypting the information transmitted over the air so that only the receivers with the correct encryption key can decrypt the information. In this paper, we studied the intrusion detection model using neural networks to accomplish the wireless network security.

Keywords: ANN, WLAN, ID system, WEP

I. Introduction

With the rapid development of communication technology, wireless communication technology has range widely, but people must bear the risks conveyed by wireless networks while enjoying the suitability brought by wireless network communication. A system called an intrusion detection system (IDS) observes network traffic for mischievous transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Intrusion Detection Systems keep track of network activity and perform thorough network analyses. They may also detect potential assaults (anomalies) as well as unwanted network access. The main problems are mainly reflected in mobile terminal problems, communication link problems, and authentication system problems.

The ANN can be considered as a data handling unit which, all things considered, looks like the working of the human cerebrum. One of these fields in which ANN has been key is cryptography. As of late there has been a significant study going on different encryption strategies in light of neural nets containing single layer or multilayer perceptron models. This field of cryptography is all the more prevalently known as Neural Cryptography. The learning strategy for ANN engineering can be very much used to produce more successful encryption frameworks in view of criticism. In the paper we studied the intrusion detection model in cryptographic simulations on how ANN can be utilized as a part of information encryption. This will help in putting a check on quantity and quality of data packets in wireless networks.

II. How does an IDS work?