Password Authentication in Wireless Networking using Neural Network Techniques

Menal Dahiya

Maharaja Surajmal Institute, Janakpuri, Delhi, India

Available online at: www.ijcseonline.org

Abstract— There are various mechanisms that provide security to the users and resources in Wireless Networking. Password authentication is one of the important procedure that enhance the security measures of the system. Drawbacks of traditional password authentication system like stolen, forgotten etc. are overcome by the technologies used for authentication mechanism like Neural Network approaches. In this paper, the two algorithms of Neural Network have been taken for conducting the experiment. Neural Network is an emerging field of Artificial Intelligence that works like a human brain. One is the Backpropagation algorithm which follows feed forward procedure and the second one is Hopfield Neural Network which works on auto associative properties of the network.

I. INTRODUCTION

Earlier computer networks were only used by the university researchers, corporate employees for sending office information through e-mail or by sharing peripheral devices among the employees in the military and in government operations [1]. At that time no one realized the security of data because the use was limited and by limited persons in a given amount of time. So security did not get a lot of attention that time. But for the last few decades, the existence of computer network spread widely. Daily, millions of ordinary people use the network facilities for their convenience such as for banking, shopping, ticket booking, watching movies online, chatting, sending emails and for the use of social networking like facebook, twitter etc. They use each and every facility of internet without knowing the security aspects. Before the widespread use of the internet, the security of information or data for an organization was provided to the managers or other reliable post and administrative means. Gradually, with the advancement in computer the need for automated tools for protecting data and other information stored in the computer became an evident basically in sharing systems. The general name given by the researchers to a collection of tools that protect data from hackers is a computer security [2]. Security is a vast topic and it includes data security and network security. Security is concerned with making sure that unwanted people cannot access or modify message intended for other recipients and unauthorized people are not trying to access the services [3]. Network security is a concept to protect data transmission over a wired or wireless network. Therefore, it is necessary to use some cryptographic methods or some other means of protection to enhance the security. Network security considers authorization of access of data in a network. Every

user assigns an Id and corresponding password that allows them to access information without any problem. This Id is the identity of its authorized usage.

Authentication is a two way process in which user confirms his or her identity to the computer system [4]. Authentication schemes are mostly based on passwords, smart cards and biometrics. Authentication ensures that the services and system resources are used by the authentic person. This paper follows the sequence of, section II describes the two different neural network approach used for the authentication of password in wireless technology. Hopfield Neural Network and Back Propagation Neural Network are the two algorithms which applied to the data to conduct the experiment. Section III describes the results and discussion followed by a conclusion.

II. PROPOSED AUTHENTICATION SCHEMES USING NEURAL NETWORKS

This section, describes the proposed procedure of user login and authentication steps by using two Artificial Neural Network Techniques:

A. Using Back Propagation Neural Network Scheme: - We propose the authentication mechanism that used Back Propagation Neural Network in wireless networking. As wireless networking requires much security measures compared to wired networking. Back Propagation Neural Network is a Feed Forward Neural Network uses supervised learning algorithm for training. The basic architecture of BPNN consists of an input layer, hidden layer and output layer. Each neuron of the input layer is connected to the hidden layer which further connected to the output layer. A

119

Performance Evaluation of Feed Forward Neural Network for Wired Equivalent Privacy/Wi-Fi Protected Access Protocols

Menal[1]* and Sumeet Gill[2]

[1]Department of Computer Science, Maharaja Surajmal Institute, Janakpuri, New Delhi - 110058, India;
menaldahiya@gmail.com
[2]Department of Mathematics, Maharshi Dayanand University, Rohtak - 124001, Haryana, India

Abstract

Objective: Millions of people use wireless devices in their day to day diligences without knowing the security facets of Wireless Technology. The aim of our research is to enhance the execution of widely used wireless devices's protocols by examining their behavior with Feed Forward Neural Network. Fundamentally, Neural Network is a multilayer perceptron network. It processes the records one at a time and "learn" by comparing the obtained output with the actual output. Hidden layer neurons play a cardinal role in the performance of Back Propagation. The process of determining the number of hidden layer neurons is still obscure. The work is focused on performance evaluation of the hidden layer neurons for WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) protocols. **Methods/ Statistical Analysis**: For this work, three network architectures have been picked out to perform the analysis. The research work is carried out by using Back Propagation Algorithm in Neural Network Toolbox on the data captured by using Wireshark tool. **Findings**: The behavior of various unlike hidden neurons is evaluated through simulation technique. Network performance is also diagnosed with the help of epochs and Mean Square Error (MSE). The performance of Neural Network is evaluated and outcomes indicate that hidden layer neurons affect the functioning of the network. **Improvement**: We would like to work with the parameter and learning of the Neural Network to achieve best results.

Keywords: Back Propagation, Feed Forward Neural Network, Hidden Layer, Mean Square Error, Wi-Fi Protected Access, Wired Equivalent Privacy

1. Introduction

Artificial Intelligence technologies like Neural Network are vastly used technology in pattern recognition. Pattern recognition is an approach which recognizes patterns and categorize data based on preliminary information or deduced numerical data from the patterns[1]. It is all about learning the behavior of machines in observing environments, discriminating patterns and building rational conclusion of the class of the patterns. This technique will

be very useful for business goals, in engineering fields or in analyzing the data etc[2,3]. Pattern recognition is the more applicable answer to all the worries related to the acknowledgement and classification of patterns like look recognition, medical examinations, speech recognition and codification of handwritten letters, figures, symbols etc. This new approach provides excess benefit or extra help in solving "real world" problems in many fields[4].

Due to the rapid advancement in the world of electronics, the wireless devices are used by millions of people

*Author for correspondence

Back Propagation Neural Network for Wireless Networking

Menal Daniya

Maharaja Surajmal Institute, Janakpuri, Delhi

www.ijcseonline.org

Abstract – The development in computers and network have changed the world very rapidly in recent years. So, the task of safeguarding the networks is very challenging. Different security algorithms and protocols have been proposed for the proper development of security mechanism. An Artificial Neural Network which is a data processing system consisting of large number of highly interconnected processing elements (neurons) in multiple layers inspired by the structure of human brain that follows a Back Propagation Algorithm can be implemented as a Wireless Network Security system. This paper demonstrates that Neural Network concept is more efficient in the area of Wireless Network Security.

Keywords: Artificial Neural Network, Back Propagation, Wireless Network

1. Introduction

Security is the term used for encompassing the characteristics of confidentiality, integrity and availability. In earlier times, two computers were together involving some physical medium running between them such as a cable [1]. But, one of the easiest and least messy ways to network computers throughout is to use the wireless technology. The problem with having the signal broadcast through a wireless network is difficult because it's tough to predict where that signal may travel. The risks to users of wireless networks have increased as the service has become more popular. In the wireless network data are transferred through radio waves spreading throughout the space and thus the information reaches anyone with the appropriate radio receiver and then easy to intercept. There were relatively few dangers when wireless technology was first introduced because it took time for intruders to find a way to crack down networks [2].

This makes a high need of secure mechanism for the protection of information in wireless network. Now-a-days there are a lot of security systems that promises to provide excellent security to user, but in spite of that many of them fail to deliver when it comes to real time testing . Due to the deficiencies in traditional password based access methods/Security systems, the new security system comes into existence which provides higher level of security. Conventionally, user authentication is categorized into three classes [3]:

- Knowledge - based
- Object or Token - based,
- Biometric - based.

The knowledge-based authentication is based on something one knows and is characterized by secrecy. The examples of knowledge-based authenticators are commonly known passwords and PIN codes. The object-based authentication relies on something one has and is characterized by possession. Biometrics technologies are gaining popularity due to the reason that when used in conjunction with traditional methods of authentication they provide an extra level of security. Biometrics involves something a person is

or does. A cryptographic system can only be as strong as the encryption algorithms, digital signature algorithms, one-way hash functions, and message authentication codes it relies on. And just as it's possible to build a weak structure using strong materials, it's possible to build a weak cryptographic system using strong algorithms and protocols which are more complex and difficult to implement. Encryption algorithms don't necessarily provide data integrity [4].

The security system using Neural Network which is suggested here is harder to be hacked. The Neural Network is used to train (learning) the identification parameters like UserID and password. Such a network acts as a brain in securing of passwords without constraints. One of the most well known types of neural network is the Multilayer Perceptron Neural Network (MLPs). Such a perceptron network makes use of Back Propagation Algorithm which is a supervised artificial neural network (ANN) [5].

The paper is organized as follows: the first section introduces the importance of security and authentication in wireless networking. Section II highlights the features of wireless networking. Next sections describe the neural network concept in wireless security, the back propagation algorithm and finally the proposed authentication method and at last paper is ended with conclusion.

2. The Leading Edge in Wireless Networking

Wireless Local Area Networks (LANs) are playing a major role in the information technology revolution. They are finding their way into a wide variety of markets including financial sectors, corporations, health care and continue to gain market momentum. The wireless networking concept is rapidly evolving, both as a technology and in the merging with adjacent technologies. The standards are surfacing in a number of areas, especially the 802.11n. The wireless networks have become popular and used widely because of few of its features that are user friendly as well as fast. Their frontiers have become ever expanding and limitless. Some of the features that popularize the wireless networks are:

- Speed and additional data download