Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 6, June 2017, pg.129 – 132

A Hopfield Neural Approach for Authenticating Password in WLANs

Menal Dahiya

Department of Computer Science, MSI, Janakpuri, Delhi, India

menaldahiya@gmail.com

Abstract— In today's tech savvy world wireless communication is the fundamental requirement of the people. Users when communicate wirelessly they did not care about the security concepts and easily trapped by the intruders. Therefore, building security between the two parties within the network is the most challenging concept. Many solutions have been provided by the researchers year by year. Sixth generation of computer come up with the Artificial Neural Network and Hopfield network was a breakthrough in Neural Network. This network gave a powerful strength to neural network's research. Their ability to learn by example makes them very flexible. They are also very well suited for real time systems because of their parallel architecture. In this paper, Hopfield Neural Network is trained to store the passwords. The passwords which are easily decrypted by the hackers are stored in the form of network parameters and other neuronal functions on the server which are difficult to hack by the intruders. This paper describes that Artificial Neural Networks will provide solution to the problem of authenticating passwords in WLANs.

Keywords —Authentication, Artificial Neural Network, Decryption Wireless Communication, Hopfield Neural Network, WLANs.

I. INTRODUCTION

Since mid 2000's the wireless communications have become extremely extensive than anyone could have thought up when it was first started. The widespread adoption of wireless technologies was speedup when authorities all over the world presented increased competition and new radio spectrum licenses for private communication assistances. The wireless communication is robust in nature and viable voice and data transport mechanism. New standards and technologies are implemented to allow wireless network more flexible as compared to wired systems. Wireless systems have been more adopted as a substitute for wired networks inside houses as well as within organizations [1]. Actually, Wireless Communications were started, especially for military purpose, but when the features and advantages of wireless communication are observed by the society then gradually this technology takes a high pace to increase. Wireless systems are now popular in the world to help society, personality, machines and organizations to communicate with each other irrespective of their location and connected wires. The easy availability of wireless networks for users is the major boom of this technology. Various security threats and attacks also attach to its working, but for the users these all are secondary issues [2]. Customers ignore these issues and take the advantage of technology. The environment, services and applications provided on the computer network nowadays leads to the risk and major threats like denial of service attack, eavesdropping, replay attacks, spoofing, hacking, etc [3]. In market, various solutions are present to overcome these problems like antivirus, intrusion detection systems, firewalls as well as many private organizations hire special network security analyst person whose job is to take care of all the security

related task and detecting threats and other malfunctioning of the network. Some organizations develop their own tools and techniques in order to protect the infrastructure of the organization and support the environment from unwanted access. The excessive usages of the internet in recent years affect the life of society very much. Everything is connected to the internet from buying vegetables to education, paying bills, for defence services and so on [4]. Networking accessibility is easy, fast and economical for everyone with continuous advancement in wireless networking; it provides easiness and convenience to the users.

Wireless networking easily merges with other network components and transfer of information take place through the air using radio waves. So, if the sender is not taking care of his message, then it is easy for the others that they alter the existing message. The risk of threats and security is more in the wireless networking because the present generation totally depends on the internet services [5]. Our requirement for internet increasing day by day, that is why protection requires. More users connect to the network; some anti-social elements also attract towards it, so protection of network needs major safety measures [6]. We need it because a single unnoticed vulnerability can lead to a destructive action in any organization. Every organization wants to protect its important figures from intruders or hackers and permit only authorized users to access the network. In recent years Soft Computing has emerged as a growing technology, with successful applications in many fields. Artificial Neural Network is one of the major tool of Soft Computing and applicable on various applications [10]. The wide areas of these applications are pattern recognition, pattern association, pattern classification etc.

In the present work, techniques of Artificial Neural Network are applied and used for analysis of wireless security. Pattern recognition technique and the Hopfield Neural Network have been used for analysis and in memorizing the input data. Here, the password keys or link keys are memorized during the training of Neural Network for a given set of data. The mechanisms or models are successful in recognising the patterns for which training was given. As the availability of wireless devices and networking become ubiquitous, the security establishment scenarios between wireless communications are necessary. This paper explores the security vulnerabilities in wireless networking and provides the necessary improvements over the security system. We have described the problems appear in the wireless network and devised the solution to them by applying artificial neural network techniques in the wireless network environment. The aim is to sparkle the awareness that how our daily wireless communications are insecure and hackers easily utilized our data or resources.

II. AUTHENTICATION METHODS IN WLANS

Authentication is a two way process in which user confirms his or her identity to the computer system [7]. There are three major types of authentication methods used by various enterprises such as Biometric based authentication which uses physical and behavioural traits of a human being, Token based authentication which uses PIN, passwords as a authentication criteria and finally Knowledge based authentication method which uses password as a key for authentication but in the form of both text and image. Along with these well known methods following are also the authentication methods which are applicable on wireless network [8].

A. Open Authentication

It is the simplest method and requires only SSIP used on the network; as long as SSID is known then the device will be allowed onto the network. The only problem with this method is that the password of the network can be easily figure out with capturing techniques.

B. Shared Authentication

This method uses a preshared key for authentication by both sides of the connection. This method is mainly suitable for small businesses.

C. EAP (Extensible Authentication Protocol)

This is the most common method used by enterprises where it utilizes an authentication server that is queried for authentication.

III. ARTIFICIAL NEURAL NETWORK

There are two problem solving technologies that deal on different models and behaviour. Soft computing is one of them. Soft computing uses a combination of Genetic Algorithm, Neural Networks, and Fuzzy Logic. A hybrid technique i.e. GA and NN or NN and FL or GA and FL would inherit all the advantages; but won't have the less desirable features of a single component [9].

An ANN may be a processing model which emulates the human mind and inspired by the way biological neurons system processes. The fundamental nature of ANN is the structure of its information processing system. ANN composed of large number of interconnected processing elements known as neurons

working simultaneously to solve a specific problem. ANN, like people learn by example. These neurons connected through weights to the other processing elements or to it. The topology of these processing elements and their interconnection are important for an ANN. The arrangement of neurons to form layers and patterns is called network architecture.

An associative memory (AM) can store the set of patterns as memories. AM is trained with a key pattern, when tested it responds by producing one of the stored patterns, which loosely relates to the key pattern. The Hopfield model is an associative memory model. This model is coined by John Hopfield. Hopfield model consists of a single layer of processing elements where each node is connected to every other node in the network, other than itself [10]. The connection weight matrix W of this network is square and symmetric. Working of this network is same as feed forward network but fast training is possible here. Here a set of patterns is taken as input and performs the training. After completion of training the network will be tested. In testing it takes a pattern and produces the output. If both are same then it means that pattern is recalled.

IV. EXPERIMENTAL SETUP

The process of adjusting weights so that network can recognize the patterns is called learning. HPNN takes a pattern as input and adjusts its weights pattern. If both are the same then it is a authentic pattern or we can say that its authentic password then user will be connected to the server. In Hopfield Neural Network, passwords are first converted into binary and then in bipolar form. For simulation purpose, we take 8 passwords for training scenarios and store their output. For testing phase, we take 4 passwords out of eight pattern sets. Output network compares the output of the network with these four patterns, if both are same then it shows that the passwords are already stored and are of authentic users.

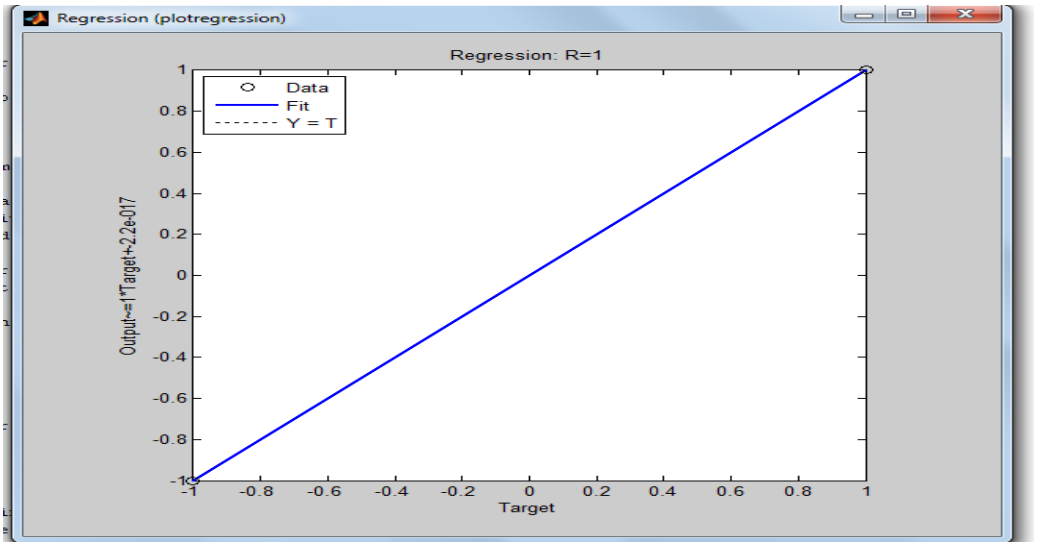
A. Training Using Neural Networks

Input training data set is [menal, mena2, India, cute3, ashish, 6vasu, #renu1, wires]

TABLE 1

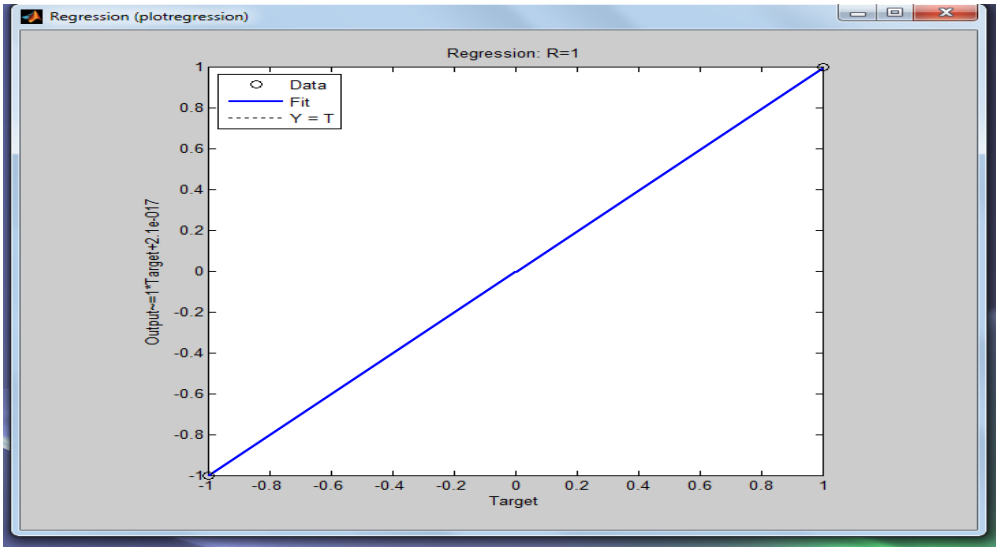
The Parameters used for The Training of Hopfield Neural Network.

Parameter	Value
Neurons in Input Layer	40
Neurons in Output Layer	40
Total Number of Patterns	8
Minimum Error Exists in the Network	12
Training Time	0.000002sec
Initial Weights and Biased Term Values	Values between 0 and 1



Graph 1: Regression Graph of all the Passwords (8) of the Network.

Input testing data set is [India, ashish, 6vasu, #renu1]



Graph 2: Regression Graph of Testing Passwords (4).

The above graph 1 shows that all the eight passwords stores in the network successfully or trained the network with the above given passwords. The testing phase randomly takes four passwords and match with the stored patterns. The straight regression line of network in graph 2 shows that the four passwords are already in the network.

V. CONCLUSION

The present work demonstrates the usefulness of Hopfield neural network based password authentication scheme successfully in a Wireless LAN networking environment. The proposed authentication approach could recall all the stored legal users accurately. There are some limitations also while using this approach or using Hopfield neural network that if more patterns are used then the stored patterns become unstable and sometimes it can misinterpret the corrupted pattern. Our future work will be checking out the maximum stored pattern capacity of the network.

REFERENCES

[1] N. Prasad and A. Prasad, *WLAN Systems and Wireless IP for Next Generation Communications*, 1st Edition, Artech House Inc, Norway, USA, 2002.

[2] I. Mohammad et al., "A Review of Types of Security Attacks and Malicious Software in Network Security," *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.4, Issue.5, pp. 413-415, 2014.

[3] N. Leavitt, "Mobile Phones: The Next Frontier for Hackers?," *Computer*, Vol.38, Issue.4, pp. 20-23, 2005.

[4] M. Rouse. (2010) Wireless LAN (WLAN or Wireless Local Area Network). [Online]. Available: http://searchmobilecomputing.techtarget.com/definition/wireless-LAN.

[5] J. C. Chen et al., "Wireless LAN Security and IEEE 802.11i," *IEEE Wireless Communications*, Vol.12, Issue.1, pp. 27–36, 2005.

[6] I. Stojmenovic, "*Handbook of Wireless Networks and Mobile Computing*," Student Edition, Wiley, USA, 2006.

[7] M. Dahiya, "Password Authentication in Wireless Network Using Neural Network Techniques," *International Journal of Computer Science and Engineering*, Vol.4, Issue.9, pp. 119-122, 2016.

[8] W. Stallings, "*Cryptography and Network Security: Principles and Practice*," Fourth Edition, Prentice-Hall Inc, 2005.

[9] D. Kriesel. (2007) A Brief Introduction to Neural Networks. [Online]. Available: http://www.dkriesel.com/en/science/neural_networks.

[10] S. N. Sivanandam and S. N. Deepa, "*Principles of Soft Computing*," Second Edition, Wiley-India, New Delhi, 2011.

