IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-4 E-ISSN: 2347-2693

Back Propagation Neural Network for Wireless Networking

Menal Dahiya

Maharaja Surajmal Institute, Janakpuri, Delhi

www.ijcseonline.org

Received: Mar/26/2016 Revised: Apr/04/2016 Accepted: Apr/22/2016 Published: Apr/30/ 2016

***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

- Availability of Better methods to secure transactions
- User mobility
- Easy sharing of resources
- Integration of more functions to a single handheld device
- Variety of devices - more and better options for users to choose
- Easy connectivity
- Usage of Self- healing techniques
- Flexibility and scalability
- Relatively low price

It is actually difficult to say why using wireless networks can be unsafe when it is the most efficient and flawless way of communicating with much less fuss. At the same time it is again tough to say when intrusions started and intruders and crackers began to access information when transmitted through wireless networks [6]**.** Security has become a major issue for every organisation.

There are number of attacks that wireless network may face. Few of such that can make wireless network unsafe are:

1) Denial of service
2) Rogue access points
3) Spooling
4) Helvetica
5) War chalking
6) Unauthorized access
7) Man-In-Middle attack

3. Neural Network's Features Suitable for Security Design

Neural network has the **property of learning**. Given a specific task to solve and a class of function, neural network can use a set of observations to solve the task in an optimal sense. Generally, according to learning task, learning ability of neural network can be classified into two main categories, i.e. supervised learning and unsupervised learning. Supervised learning is the learning with a 'teacher' in the form of a function that provides continuous feedback on the quality of solutions. These tasks include pattern classification, function approximation and speech recognition, etc. Unsupervised learning refers to the learning with old knowledge as the prediction reference. These tasks include estimation problem, clustering, compression or filtering. It is easy to compute the output from the input while difficult or impossible to compute the input from the output. In neural network, there are often more inputs than outputs. This is called the **one way property** of Neural Network.

4. Neural Network in Wireless Security

Wireless Networks are used to connect users to wired structure of a corporate network because Wireless Networks are directly associated with the core network of the corporation, security is a critical factor in the management of the network. One of the basic needs of Wireless Networks is effective security against intruders.

An unauthorized access on a system that violates the security mechanism is called intrusion. Intrusion detection is the process that is used to identify individuals who are using a computer system without authorization and those who are legitimate access to the system but are exceeding their privileges. Intrusion Detection (ID) has been the active field of research for about two decades. Various detection techniques are searched for attack patterns in the design of intrusion detection systems. Still, despite of active research and commercial investments, ID technology is immature and its effectiveness is limited. This problem can be handled by ANN techniques. ANN provides a platform that can be enhanced with other SC techniques to detect and prevent network intrusions and other related attacks.Artificial Neural Networks are a non-algorithmic approach to information processing inspired by the biological nervous systems. Wireless applications are inherently nonlinear in nature. The non-linearity associated with wireless makes ANN more robust and effective than conventional linear procedures in wireless networks. The most important property of a Neural Network is to automatically retain coefficients according to data inputs and data outputs. Here, we explain the Back Propagation Neural Network method.

4.1 Proposed Authentication Method is based on Neural Network

The objective of developing authentication system can be fulfilled by means of applying the suitable learning of password and developing an appropriate architecture. For secure authentication, we would train the network. For this, there are number of training algorithms available in Artificial Neural Network such as:

- Back Propagation Network (BPN)
- Resilient Back Propagation Network (RBPN)
- Radial Basis Function network (RBF)
- Hopfield Neural Network (HNN),etc.

Among all these, BPN is most useful for Feed-Forward type of Neural Networks. This section will contain details about architecture of neural network, learning rule, target definition and process, which will apply for authentication.

Back Propagation Neural Network method:

The Back Propagation method is a technique used in training multilayer neural networks in a supervised manner. The Back Propagation method, also known as the error back propagation algorithm, is based on the Error-Correction Learning rule [7]. It consists of two passes through the different layers of the network: a forward pass and a backward pass. In the forward pass, an activity pattern is applied to the input nodes of the network, and its effect propagates through the network layer by layer. Finally, a set of outputs is produced as the actual response of the network. During the forward pass the synaptic weights of the networks are all fixed. During the backward

pass, the synaptic weights are all adjusted in accordance with an error-correction rule. The actual response of the network is subtracted from a desired response to produce an error signal. This error signal is then propagated backward through the network. The synaptic weights are adjusted to make the actual response of the network move closer to the desired response in a statistical sense. The weight adjustment is made according to the generalized delta rule [8] to minimize the error.

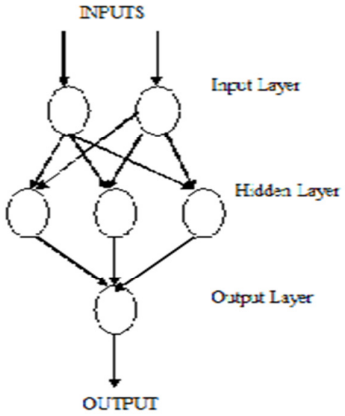

Fig.1 Feed forward architecture

Two commonly used neuron activation functions for the neuron are sigmoidal and tansig functions. Both functions are continuously differentiable everywhere and typically have the following mathematical forms:

Sigmoidal: $f(x) = \frac{1}{1+\exp(-ax)}$, a > 0

Tansig: $f(x) =$ a tanh(bx), a&b > 0

Most common form of authentication use today are UserID's and passwords. These inputs converted into binary equivalent and encode through the encoder. When we implement Neural Network the encoded UserID is taken as an input to the BPN and produces an output. Then this output is compared with the encoded password which was entered by the user. If they match, the Login is successful else the access is denied.

Input (User ID) = Output (Password)

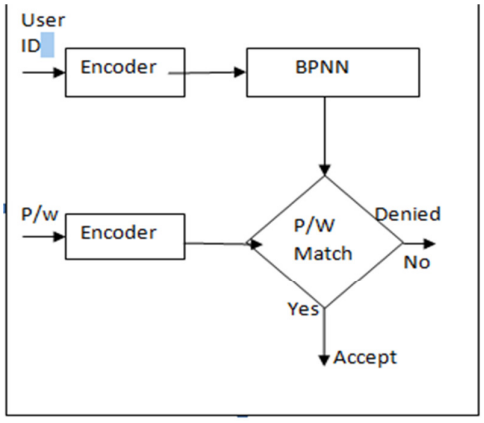

Fig.2 Block Diagram for proposed authentication system

5. Conclusion

This proposed authentication method is based on the concept of neural networks. Here, the trained network generates outputs that are exactly identical to desired outputs. If user inputs wrong combination of username and password, it rejects as an unauthorized user. The reason is that each username and password has been registered in the system and has been used to train the neural network. After training, the applied data are converted to the weight values that cannot be easily hacked by an intruder. So, this system can be used to securely store the passwords. In summary, neural networks offer a unique way to solve some problems while making their own demands. Neural Network approach introduces a new ray of light in this field. Wireless Networks need to employ latest methods of security so as to ensure users that their transactions are completely safe. The password based security system will get a new direction of development. There is a very good scope to enhance the level of security using Artificial Neural Network.

References

[1] M. Mathis, J. Heffner, P. O'Neil, P. Siemsen, "Pathdiag: Automated SVChosting", PAM 2008.
[2] J. C. Honig, D. Katz, M. Mathis, Y. Reckhter and J. Y. Yu, "Applications of database chaining in the Internet", RFC1164 USC/Information Sciences Institute, June 1990.
[3] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of IEEE, Vol. 91, No. 12, pp. 2019-2040,Dec 2003.
[4] Bruce Schneier**, "**Security Pitfalls in Cryptography**"** 1998**.**
[5] Lin, I., OU, H. & Hwang, M. (2005). A UserAuthentication System Using Back-Propagation Network. Neural Computing and Applications, 14, 2005, PP. 243-249.
[6] R. L. Clay, J. Mahdavi, G. J. McRae, "Scheduling in the Presence of Uncertainty in database chaining. The Linear Assignment Problem," Proceedings of AICHE National Meeting, August, 1991.
[7] J. Principe, N. Euliano, W. Lefebvre, "Neural and Adaptive System: Fundamentals through Simulations", Wiley, 2000, ISBN: 978-0-471-35167-2
[8] S. Haykin, "Neural Networks – A Comprehensive Foundation", Prentice Hall, 2nd edition 2000. ISBN: 0132733501
[9]www.it.iitb.ac.in/~palwencha/assg/wlan_sec.pdf www.ece.tamu.edu/~reddy/ee689.../indira-monica.pdf
[10 wireless-technology-advisor.com/ wireless- technology-trends .html
[11]www1.cse.wustl.edu/~jain/cse574- 06/ftp/j_2trn.pdf
[12]www.afn.org/~afn48922/downs/wireless/wireless_wan.pdf

Author's Profile

Menal Dahiya: Is Assistant Professor in the Department of Computer Science and Applications, Maharaja Surajmal Institute, Delhi. M. Phil (computer science) and currently pursuing Ph.D. Her research interests are in the area of Wireless networks, neural networks and computer network security. She has published some papers on these topics.

