International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 3 (2017), pp. 321-326

http://www.ripublication.com

Framework For Wireless Network Security Using Hash Function Based On Feed Forward Artificial Neural Network

Menal
Assistant Professor, Dept. of Computer Science,
MSI (GGSIPU), Janakpuri, Delhi, India.

Abstract

Every time computer user asked to keep secret their passwords for various purposes. But memorization of all the passwords always is a tedious job. In this paper, we construct a Hash Function based on Feed Forward Neural Network. Hash Function is one way and secure against Man-in-the-Middle attack. Wired Equivalent Privacy is a well known Wireless Protocol used by every wireless communication user. We try to enhance the security of Wireless Communication by making the WEP protocol password more strong. The network parameters of Feed Forward Neural Network act as a secret key for generating the Hash Function.

Keywords: Feed Forward Neural Network, Hash Function, Wired Equivalent Privacy, Wireless Communication.

INTRODUCTION

Wireless Network transfers large amounts of data daily which is confidential, sensitive and vulnerable to attacks. Mostly in all the fields wireless communication saw widespread growth over the last few years. Wireless communications regularly expand and show a continuous growth in the cellular telephone, mobile networks, Wireless Internet and in home networking. Many mobile devices store data and a good amount of bandwidth connectivity is achieved even when they travel [1]. Users could use their laptops and granted access to different networking resources. With so many advantages of wireless networking, some form of security is also necessary to prevent unauthorized access to connected resources. Over time, many solutions to security threats have been introduced, some of them were applied and some are replaced by security standards. This continuous process of security enhancements

promoted the security field to be a permanent research topic. Use of encryption and decryption technologies are the fundamental security solutions and their weaknesses are well known to attackers.

Cryptography is the mechanism which prevents the information from others. Therefore, maintaining the authenticity and integrity of the information is the basic need in computer networks [2]. As alone Cryptography is not a sufficient solution for network security. We therefore combine Neural Network with Cryptography to achieve an enhancement in wireless security. The hash function encodes a variable length message and give out a fixed length size output, known as a Hash code of the message or message digest of the message [3]. Hash code provides an error detection capability as if there is a change in any bit of the message, then it affects the message hash value and the result is in a change to the Hash code. A secure Hash code is very much important for the satisfaction of various requirements such as security against birthday attack, man-in-the-middle attack and one way property. Some of the widely used Hash functions are SHA, MD5, HMAC etc. [4]. These Hash functions are not satisfying the security of information fully. Thus, the requirement of new Hash function is arise. Confusion and diffusion properties of Neural Networks have been used to design encryption algorithms such as stream cipher or block ciphers [5]. Neural Network is non-linear in nature and most of the researchers applied this property as an alternative to the hash algorithm. Like Hash function Neural Networks have also a one way property which helps in designing Hash function.

In order to make the framework of wireless network security, we should carefully handle the key management protocol. We therefore, try to design a secure framework for wireless network using Hash function based on Neural Network. The paper consists of explanation of wireless communication and protocols in section II, section III comprises of a proposed Hash function and then the conclusion of the paper.

OVERVIEW OF WIRELESS NETWORKS

The broadcasting nature of radio wave propagation in the air interface is open to every user whether it is legal or illegitimate users. Signal propagation in case of wired network is secure at the first time as the communication devices are physically connected to the network. There is totally a different scenario in case of wireless network. The open environment of wireless is vulnerable to various passive and active attacks. Apart from this drawback, during the past decades wireless communication usage and services have been accelerated with a high pace and achieve the goal of meeting the increased demand [6]. According to the latest survey in 2013 by International Telecommunication Unit (ITU), the number of mobile users has reached 6.8 billion and almost 50% of the world's population is using the internet. A large part of the population uses wireless networks by making hotspots, rogue access points or by unauthorized access without even know the consequences of using wireless network without or less security. Wireless network faces a big challenge in case of providing the protection against accessing the network from unwanted users and also

to provide security to the user's private data [7]. The general security issues in wireless networks are Confidentiality, Integrity and Availability.

In order to provide authenticity and security wireless networks include authentication protocols and cryptographic algorithms to secure the communication. Wireless networks employ a different authentication mechanism at different protocol layers. At the network layer, the Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access2 (WPA2) are the commonly applied protocols in the Wireless Networking [8]. These protocols provide privacy for the user's information that's transferred from sender to receiver through encryption access the network. Table 1 shows a brief overview of wireless security protocols.

Table 1. Summary of Wireless Protocols

WEP (Wired Equivalent Privacy)	40-bit key for Encryption	Easily Broken Security Algorithm with Numerous Flows
WPA (Wi-Fi Protected Access)	128-bit key for Encryption	Uses Pre-shared Key (PSK) and Temporal key Integrity Protocol (TKIP)
WPA2 (Wi-Fi Protected Access version2)	128,192,256 bit Keys for Encryption	Uses Advanced Encryption Standard (AES)

PROPOSED HASH FUNCTION BASED ON NEURAL NETWORK

The architecture of Feed Forward Neural Network consists of of number of layers, namely input, hidden and output layers. When flow of data is from input to output unit, then it follows feed forward network architecture [9]. For the purpose of one way hashing function, we take simple three layer network, the first layer is the input layer, then hidden layer and finally the third output layer. The network may contain more than one hidden layer according to the condition. All layers are connected serially input bits are fed into the hidden layer and output of a hidden layer is fed into the output layer. We take 64-bit WEP key of a wireless device as an input of the network. All the input values are in binary form either 0 or 1. Due to sigmoid function, the output of the network is between 0 and 1. The value of the weights and biases are generated randomly. For satisfying the concept of one way hash function, the value of the weights is required to be the same every time the network is initialized.

The structure of the feed forward network implemented in this paper has an output layer of 64 nodes, with a hidden layer consisting of 24 nodes and number of input bits is 64. After determining the neural network parameters, the network weights to be initialized randomly and then train the network. The fee forward network can be represented in matrix form as:

$$\begin{pmatrix} W_{1,b} & W_{1,0} \cdots\cdots\cdots\cdots W_{1,63} \\ W_{2,b} & W_{2,1} \cdots\cdots\cdots\cdots W_{2,63} \\ \vdots & \\ W_{24,b} & W_{24,1} \cdots\cdots\cdots\cdots W_{24,63} \end{pmatrix} X \begin{pmatrix} 1 \\ i_0 \\ \vdots \\ i_{63} \end{pmatrix} = \begin{pmatrix} O0 \\ O1 \\ \vdots \\ O_{63} \end{pmatrix}$$

$$\begin{pmatrix} W_{i,b} & W_{1,0} \cdots\cdots\cdots W_{1,23} \\ W_{2,b} & W_{2,0} \cdots\cdots\cdots W_{2,23} \\ \vdots & \\ W_{64,b} & W_{64,1} \cdots\cdots\cdots W_{64,23} \end{pmatrix} X \begin{pmatrix} 1 \\ O0 \\ \vdots \\ O_{63} \end{pmatrix} = \begin{pmatrix} Y0 \\ Y1 \\ \vdots \\ Y_{63} \end{pmatrix}$$

Where Y_0 to Y_{63} is the result of the output layer, $W_{x,y}$ is the weight corresponding to neurons and O_0 to O_{23} is the result from hidden layer. As the output of the Neural Network tends to be a real number, each derived subkey bit is considered to be 0 or 1. The derived key becomes the input key for the plaintext to be encrypted. This key can be used with any encryption algorithm for transmitting the messages. For variable size password P, a fixed size output generates, referred to as hash code H (P) [10]. The key generated is about 64 bits which is further divided into four parts of 16 bits each. These four keys generate subkeys that are used to determine the input to the neural network to obtain the hash code. Three layer feed forward neural network is used for generating hash function. These layers are used to realize data confusion, diffusion and compression respectively [11]. First of all password P is divided into n number of blocks each of 16 bits. Before applying neural network XORed them.

$$P = P_1 \text{ XOR } P_2 \text{ XOR} \ldots . P_n$$

Then the input layer is defined as:

$$X = f^T (\sum W_{0,i} P_i + B_0, Q_0)$$

Where W is the weight vector from $w_{0 \ldots\ldots} w_{16}$, i=0 to 16 f^T is the transfer function and denotes the iteration time, B is the bias and Q is the control parameter. The repeated iteration increases the strength of cryptosystems.

Hidden layer is defined as:

$$O = f_1(W_1 X + B_1, Q_1)$$

And the final Hash value is obtained as:

$$H = f_2(W_2\ O+B_2,Q_2)= f^T(W_2\ O+B_2,Q_2)$$

It means that T time a transfer function is iterated. For computing P, we require weight and bias of the network, but they are not known.

CONCLUSION

In this paper, we proposed and analyzed a Hash Function generated by Neural Network. A three layer neural network architecture is presented for the construction of Hash Function. Kulkarni et al. to generate one way Hash Function along with a piecewise linear chaotic map. They analyzed that this hash function is high key sensitivity and plaintext sensitivity. Later on Soni et al. implement the Hash Function based on Neural Cryptography with piecewise linear chaotic maps for data protection. They compare cryptographic hash functions with neural hash function. We design an efficient Neural Network based Hash Function which uses the hash algorithm for wireless security. WEP key has numerous flaws in its encryption method and so less secure. This neural hash function follows one way property so, a slight change in the initial weight values of the network results in the totally different hash output. Structure can be modified by adding more neurons in each layer and it will be the best choice for data authentication.

REFERENCES

[1] O.Aliu, A.Imran, M.Imran, B.Evans, "A Survey of Self Organisation in Future Cellular Networks", IEEE Communication Surveys & Tutorials, Volume.15, Issue.01, pp. 336-361, February 2013, DOI: 10.1109/SURV.2012.021312.00116.

[2] William Stallings, "Cryptography and Network Security: Principles and Practice-Third Edition", Pearson, August 2002, ISBN: 978-0130914293.

[3] Shiguo Lian, Jinsheng Sun, Zhiquan Wang, "One way Hash Function Based on Neural Network", Journal of Information Assurance and Security, 2006.

[4] S.A.Vanstone, A.J.Menezes, P.C.Oorschot, "Handbook of Applied Cryptography", CRC Press, October 1996, ISBN: 0-8493-8523-7.

[5] L.P. Yee, D.L.C. Silva, "Application of Multilayer Perceptron Network in Symmetric Block Ciphers" International Joint Conference on Neural Networks, Volume. 02, Issue.12-17, pp. 1455-1458, May 2002.

[6] S. Santra, P P. Acharjya, "A Study and Analysis on Computer Network Topology For Data Communication", International Journal of Engineering Technology and Advanced Engineering, Volume.03, Issue.01, pp. 522-525, 2013.

[7] T. Godhavari, N.R. Alamelu, R. Soundararajan, "Cryptography Using Neural Network Annual IEEE INDICON, 11th-13th December 2005, DOI: 10.1109/INDCON.2005.1590168.

[8] Radomir Prodanovic, Dejan Simic, "A Survey of Wireless Security", Journal of Computing and Information Technology, Volume.15, Issue.03, pp. 237-255, January 2007.

[9] Simon Haykin, "Neural Networks: A Comprehensive Forndation-First Edition", Prentice Hall PTR, 1994, ISBN:0023527617.

[10] V.Soni, S.Tanwar, K.V.Prema, "Implementation of Hash Function Based On Neural Cryptography", International Journal of Computer Science and Mobile Computing, Volume.03, Issue.04, pp. 1380-1386, April 2014.

[11] V.R.Kulkarni, S.Mujawar, S.Apte, "Hash Function Implementation Using Artificial Neural Network", International Journal on Soft Computing, Volume.o1, Issue.01, November 2010, DOI: 10.5121/IJSC.2010.1101.