International Journal for Modern Trends in Science and Technology
Volume: 03, Issue No: 03, March 2017
ISSN: 2455-3778
http://www.ijmtst.com

Neural Cryptography for Secret Key Exchange

Prof.Pranita P.Hadke[1]| Prof.Madhuri R. Dubey[2]

[1] Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India.
[2] Department of Information Technology, SBJITMR, Nagpur, Maharashtra, India

To Cite this Article
Prof.Pranita P.Hadke and Prof.Madhuri R. Dubey, "Neural Cryptography for Secret Key Exchange", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 03, 2017, pp. 15-18.

ABSTRACT

The goal of any cryptography system is the exchange of information among the intended user without any leakage of information to other who may have unauthorized access to it. A common secret key could be created over a public channel accessible to any opponent. Neural networks can be used to generate common secret key. In case of neural cryptography, both the communicating networks receive an identical input vector, generate an output bit and are trained based on the output bit. The two networks and their weights vectors exhibit a new phenomenon, where the networks synchronize to a state with identical time-dependent weights. The generated secret key over a public channel is used for encryption and decryption of the message or information send over the channel.

KEYWORDS: Neural networks, Cryptography, Key exchange, neural cryptography.

I. Introduction

Nowadays information security has become an important aspect in every organization. In other words people have to be assured that the information to be read by only the sender and receiver. The basic need to provide security is using cryptography. Cryptosystem are commonly used for protecting the integrity, confidentiality, and authenticity of information resources. The design of cryptography algorithm is complicated by the fact that a variety of cryptanalytic attacks are available that can often be successfully used to recover the key or the plaintext.

Cryptography has two style of encrypting data; symmetrical and asymmetrical. Symmetric encryptions use the same key for encryption and decryption process, and also can be defined as a secret-key, shared-key, and private-key. Asymmetric cryptography uses different encryption keys for encryption and decryption process. In this case an end user on a network, public or private, has a pair of key; one for encryption and one for decryption. These keys can be identical as a public and a private key.

Key generation is the most significant issue in cryptography technique. In recent times wide ranges of techniques are developed to protect data and information from eavesdropper. These algorithms have their virtue and shortcomings. A neural network based approach offers an attractive solution to this problem in that it provides a suitable framework within which data can be readily code. Neural networks are non linear statistical data modeling tools. They can be used to model complex relationship between inputs and outputs or to find patterns in data. A phenomenon of neural networks is applied in cryptography system. This is used for generating secret key.

II. PROBLEM OF SECRET KEY EXCHANGE IN CRYPTOGRAPHY

The problem of key exchange is one of the main concerns of classical cryptography and it was extensively studied in classical cryptography. The first published key exchange protocol was based on number theory and it is known by Diffie-Hellman key exchange protocol. While it depends on the difficulties of computing discrete logarithms, it is vulnerable to man-in-middle attack. Moreover, it is computationally intensive. The man-in-middle attack is solved by authentication mechanisms.

III. Related work

This paper [1] proposed two artificial neural networks for cryptography. Experimental results show that the two networks are secure, without any result about efficiency.

This paper [2] presented synchronization neural key-exchange algorithm for cryptography. The model has multi-layer feed-forward neural network which have two tree parity machine (TPM) that synchronized with a random initial weight act as common secret key for the encryption and decryption process. The weight can be updated according to the learning rules only if the output values of the two machines are equal. Throughout the synchronization process, only the input vectors and the output vectors are transmitted over the public channel.

This paper [3] presented a new modification of the Advanced Encryption Standard to be immune against some attacks using non linear neural network. The neural network model performs cryptography processes via a symmetric key cipher that used as the initial weights for the neural network which trained to its final weight fast and low cost algorithm. The objective form the network has been selected to equivalent the output of the AES that have an efficient and recommended security. Simulation results show the proximity of the result accomplished by the proposed NN-based AES cryptosystem with that of the normal AES.

This paper [4] proposed multi-layer neural networks in cryptography. The multilayer neural networks in cryptography. The multilayer neural networks modified by back-propagation. The planned model converted the input message into ASCII code then gets the sequence of bits for each code which divides into 6 bit blocks are used as input for the encryption process. The cipher key is the neural network structure contained input layer, hidden layer, output layer, and updated weights. Experimental results show that the system is secure.

This paper [5] proposed a secret key using neural cryptography, based on synchronization of Tree Parity Machine (TPMs) by mutual learning. The system has two identical dynamical system, which starting from different initial conditions and synchronized by a common input values which are coupled to the two system. The networks received a common input vector after calculating their output and updated their weight vector according to the match between their mutual outputs in every time step. The input and output relations are not exchanged through a public channel until their weight vectors are matched and can be used as a secret key for encryption and decryption of secret message. The weight vectors of the two neural networks begin with random number, which are generated by Pseudo-Random Number Generator (PRNGs). The proposed model fixed the security against numerical attacks.

This paper [6] proposed a secret key over a public channel using artificial neural network. The artificial neural network contains of two multi layer neural networks trained on their mutual output bits and able to synchronize. The two network starting from random initial weights and learning from each other with two multilayer networks relax to the state with time dependent identical synaptic weights. The partners didn’t exchange any information over a secret channel before their communication. Synchronization of neural networks can be considered as the key generation in cryptography. The common identical weights of the two partners can be used as a key for key generation over public channels which are not based on number theory. Experimental result shows that the model is fast, simple, and secure.

This paper [7] presented a secured cryptography secret-key based on neural network in a public channel. The proposed model has two neural network that are trained on their alternative output synchronized to an equal time dependent weight vector through a chaos synchronization system that starting from different initial condition. The system combined the neural network with the logistic chaotic map. The both partners used their neural networks as input for the logistic maps which generated the output bits to be learned, by mutually learning. The two neural networks approach each other and generated a matching signal to the chaotic maps. The chaotic synchronization applied in the neural cryptography enhanced the cryptography system and improved the security.

This paper [8] proposed a common secret key generated based on neural networks. The neural cryptography has two communication networks that received an identical input vector, generated an output bit and are trained based on output bit. The network model initials the weight randomly and the outputs bit are generated finally and exchange between partners. The weight may be modified if the outputs of both partners are matched. The modified weight after synchronize act as a secret key for the encryption and decryption process. Simulation results show that the cryptosystem based on ANNs is secure.

In this paper [9] a secret key is generated over a public channel based on neural network. The model has a neural network machine contains of two partners started with initial weights and different initial condition which synchronized by a common external signal and received a common random input vector and learned their mutual output bits. The synaptic weights are used as a secret key over a pubic channel. Simulation results show that the model are secure and efficiency.

IV. PROPOSED SYSTEM

Proposed Approach

1. Interacting Neural Networks and Cryptography

i. Two identical dynamic systems, starting from different initial condition can be synchronized by a common external signal which is coupled to the two systems. Two networks which are trained on their mutual output can synchronize to a time dependent state of identical synaptic weights.

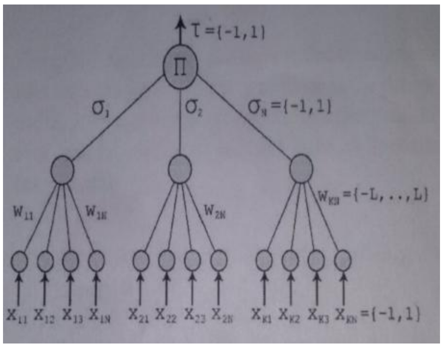
ii. This phenomenon is also applied to cryptography. Neural networks learn from examples. Training means, that synaptic weights adopt by simple rules to the input/output pairs. After the training phase the neural network is able to generalize: it can classify the input pattern which does not belong to the training set.

iii. The two patterns A and B do not have to share the common secret key but use their identical weights as a secret key need for encryption.

iv. In neural network an attacker E who knows all the details of the algorithm and record any communication transmitted through this channel finds it difficult to synchronize with the parties, and hence to calculate the common secret key.

2. Neural Key Exchange

The most used protocol for key exchange between two parties A and B in the practice is Diffie-Hellman protocol. Neural key exchange, which is based on the synchronization of two tree parity machine, should be a secure replacement.



Tree Parity Machine

3. Tree Parity Machine

Tree Parity Machine is special type of multi-layer feed-forward neural network. It consist of one output neuron, K hidden neurons and K*N input neurons. Inputs to the networks take 3 values:

xij$\in \{-1,0,1\}$

The weights between input and hidden neurons take the values:

wij$\in \{-L, \dots, 0, \dots., +L\}$

Output values of each hidden neurons is calculated as a sum of all multiplication of input neurons and these weights:

$\sigma i = sgn(\sum_{j=1}^{N} wijxij)$

Sig num is a simple function, which returns -1,0 or 1:

Sgn (x)= $\begin{cases} -1 \; if \; x < 0, \\ \; 0 \; if \; x = 0, \\ \; 1 \; if \; x > 0. \end{cases}$

If the scalar product is 0, the output of the hidden neuron is mapped to -1 in order to ensure a binary output values. The output of neural network is then computed as the multiplication of all values produced by hidden elements:

$$\tau = \prod_{i=1}^{K} \sigma i$$

Output of the tree parity machine is binary.

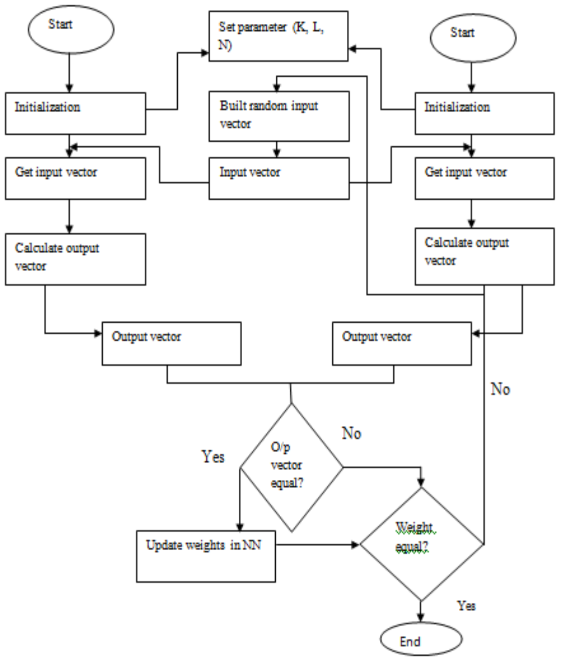
4. Secret Key Generation

The different stages in the secret key generation procedure which is based on neural networks can be stated as follows:

1. Determination of neural network parameter: K the number of hidden layers units, n the input layer units for each hidden layer unit, l the range of synaptic weight values is done by the two machine A and B.
2. The network weight to be initialized randomly.
3. The following steps are repeated until synchronization occurs.
4. Inputs are generated by the third party (key distribution center).
5. The inputs of the hidden units are calculated.

6. The output bit is generated and exchange between the two machine A and B.
7. If the output vectors of both the machine agree with each other then the corresponding weights are modified using the learning rules.
8. When synchronization is finally occurred, the synaptic weights are same for both the networks. And these weights are used as secret key.

5. Proposed Architecture



V. RESULTS

It is expected that the proposed approach make the error rate as minimum as possible and highly increase the security of data in data communication system.

VI. CONCLUSION AND FUTURE WORK

Artificial neural network is an efficient technique which has the ability to implement security using tree parity machine (i.e. special type of feed forward neural network). One of the primary aspect in this field of neural cryptography appears to be the discovery of neural architecture with very high synchronization speed, and design the encoding and entropy of the information exchanged during mutual learning, to prevent the synchronization of an attacker during the mutual learning process.

References

[1] Navita Agarwal, Prachi Agarwal, "Use of Artificial Neural Network in the Field of Security", MIT International Journal of Computer Science & Information Technology, Vol. 3, No. 1, 42-44, 2013.

[2] Ajit Singh, Havir Singh, "Cryptography for Secret Key Exchange and Encryption with AES", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 5, 376-381, 2013.

[3] Siddeq Y. Ameen, Ali H. Mahdi, "AES Cryptosystem Development using Neural Networks", Inernational Journal of Computer and Electrical Engineering, Vol. 3, No. 2, 315-318, 2011.

[4] Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek, "Cryptography based on neural network", Proceedings 6th European Conference on Modelling and Simulation, 2012.

[5] N. Prabakaran, P. Vivekanandan, " A New Security on Neural Cryptography with Queries", International Journal of Advanced Networking and Apllication (IJAIA), Vol.2, No. 1, 60-69, 2011.

[6] Wolfgang Kinzel, IdoKanter, "Neural Cryptography", Proceedings TH2002 Supplement, Vol. 4, 147-153, 2003.

[7] Einat Klein, Rachel Mislovaty, Idokanter, Andreas Ruttor, Wolfgang Kinzel, "Synchronization of neural network by mutual learning and its application to cryptography", International Proceeding of: Advances in Neural Information Processing System 17, Neural Information Processing System NIPS, 2004.

[8] R. M. Jogdand, Sahana S. Bisalapur, "Design of an efficient neural key generation", International Journal of Artificial Intelligence & Application (IJALA), Vol. 2, No. 1, 60-69, 2011.

[9] Pratap Singh, Havir Singh, "Cryptography in Structure adaptable digital neural networks", National monthly refereed journal of research in science & technology, Vol. 1, Issue. 12, 35-44,2012.

[10] William Stalling, " Cryptography and Network Security: Principles and Practicle, (5th Edition), Prentice Hall, 2010.

[11] M. Arvandi, A. Sadeghian, "On the use of Recurrent Neural Networks to Design Symmetric Cipher", IEEE Computational Intelligence Magazine, pp. 42-53, May 2008.

[12] Khalil Shihab, " A back propagation Neural Network for computer Network Security", Journal of computer science 2(9): 710-715, 2006.

[13] Behrouz A. Forouzan, " Cryptography and Network Security", Tata McGraw-Hill, Special Indian Edition, 2007.

[14] Meghdad Ashtiyani, Soroor Behbahani, Saeed Asadi, Parmida Moradi Birgani, " Transmitting Encrypted Data by Neural network", 2007 IEEE International Symposium on Signal Processing and Information Technology, pp. 385-389, 2007.

[15] Seref S. Neclao, " Neural Solution for Information Security", Politeknik Dergisi, Journal of Polytechnic, Vol. 10, No. 1, 21-25,2007.