Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FL2440 HARDWARE BASED NEURAL DATA SECURITY USING POLARIZATION ENCRYPTION (E_P) APPROACH

[1]KULDEEP CHOUHAN, [2]DR. S. RAVI

[1,2]Dr. MGR Educational and Research Institute University, Chennai

Email: kuldeep0009@gmail.com , ravi_mls@yahoo.com

ABSTRACT

Encryption scheme is widely used in the field of communication network security. The network systems are focus on reliability, service and functions, which provided end-to-end service to protect encrypted data node. It enables to interconnect the various functional levels to interact and communicate with each other. An interconnected group of nodes use a computational model for data processing, which is based on a node connections approach. In this work, data are transmitted from 'n' inputs as packets (e.g. 1 byte), through hardware based E_P, shows polarized output after checking bits. Similar, process is followed to make sure for encrypted data for another in node clusters is proposed. An experimental setup is done with python based polarised NN output to check whether testing phase of bits is enable to check an error during training process is also presented.

Keyword: *Data Security, Polarization Encryption, FL2440 Hardware Board, Cluster Of Nodes*

1. INTRODUCTION

The node authentication is increasing lots of attention and requires providing security in different layers of the network [1,2]. It also has to improve the confidentiality and data availability [5]. Wireless networks consist of data nodes with limited computational and communication capabilities [10]. The advanced technologies and information management systems are more powerful and enforcing information security becomes more critical [3,11]. The huge use of the communication networks for various purposes developed many new serious security threats with increased violations in the internetworking world [17]. Secrecy is compromised if information is disclosed to users not authorized to access it. The E_P scheme used in the work is based on data security and implemented using neural network technique.

1.1 Polarization Encryption Scheme for Data Security

The encryption and polarization encryption have attracted much attention recently and have ability to perform high space-bandwidth product, as well as obtaining real-time encryption to unauthorized decryption and its portability [8]. Moreover, an encryption has the possibility of supporting biometric based approaches also. The polarization encryption (E_P) provides additional flexibility in the key encryption design by adding a polarization state manipulation to the phase and amplitude manipulation (conventionally used in optical encryption methods) and makes E_P method more secure.

2. COMMUNICATION NODE NETWORKS BASED ON ENCRYPTION TECHNIQUE

Communication node networks should be able to understand the security and communication environment to make decisions and manage network resources efficiently [16,19]. The security network system needs to include the ability to recognize user, service provider and infrastructure [7]. The appropriate action is to increase the optimal and efficient use of network resources in delivering high-quality services [15,20]. The different types of network layers, which are necessary for a secure network adaptation process includes,

(i) End-User layer
(ii) Subscriber layer
(iii) Control layer
(iv) Network polarised encryption layer

3. METHODOLOGY

A process or state in which data exhibit different properties in different node directions and each node data can encrypt and transmit Figure 1 shows the polarised bits formed after encryption.

Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Original Signal	1	0	1	1	1	0	1	0	0
Polarised Signal	$	#	$	$	$	#	$	#	#

Figure 1: Schematic of Polarization Encryption

In this section, two different types of rule processes are followed to keep data secure among cluster of nodes,

Rule$_1$: Randomness in selecting the bits that correspond to base zero and base one, and

Rule$_2$: Inserting the check bits into the data at random positions.

As an example, two different positions for check bits interleaved with the data are shown in Figure 2 and Figure 3 shows the infinite positions are possible in realtime.

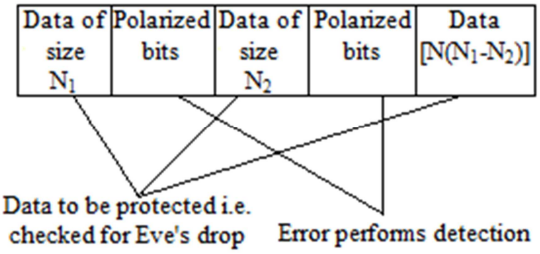


Figure 2: Different positions for the check bits interleaved with data

(Data) N_1	Polarized bits	Polarized bits	Data (N-N_1)

Figure 3: Polarized bit for neural data in the frame

The data structure includes,

(i) Size of the check bits
(ii) Base selected for bit zero and bit one
(iii) Position of the check bits in the frame

The above are mutually agreed between Tx: and Rx:

Figure 4 shows the flow of data between Tx: and Rx:

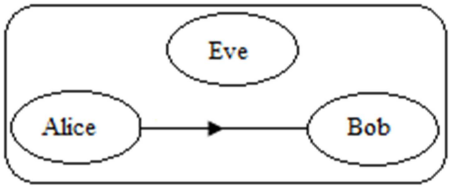


Figure 4: Information exchange between two data nodes

The encrypted data is shared among trusted users, and decryption requires,

(i) Size of the key
(ii) Position of the key
(iii) Base, used to generate the key

The data structure is shown in Figure 5.

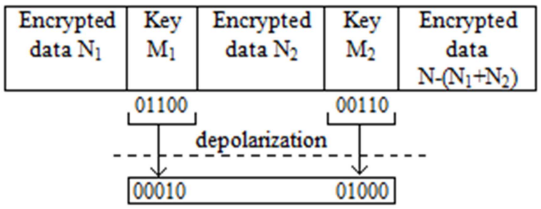


Figure 5: Encrypted data bits and depolarized key

The receiver will decrypt the encrypted data using the depolarization scheme shown in Figure 6 and Figure 7.

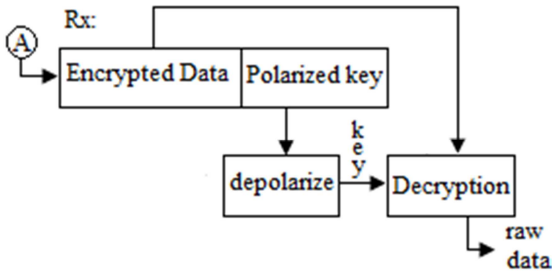


Figure 6: Depolarize scheme and decryption of data

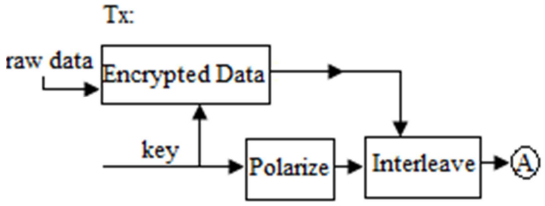


Figure 7: Encryption using Polarization of data at Tx:

3.1 Polarization States for Network Node Transmission Scheme

The polarization state source has terms of four parameters $\{P_0, P_1, P2, \text{and } P_3\}$ and the total intensity is P_0 while P_1, P_2, and P_3 describe the polarization state. It is determined by measuring the intensity of transmission speed after passed through various optical elements. The last three parameters $\{P_1, P_2, \text{and } P_3\}$ mapped conveniently and represent for all polarization states. In terms of the polarization sphere, the different parameters are mapped as,

$P_0 = I$ = total intensity of the beam
$P_1 = Ip\ cos(2\chi)cos(2\psi)$
$P_2 = Ip\ cos(2\chi)sin(2\psi)$
$P_3 = Ip\ sin(2\chi)$
$P_0 = \{(P_1)^2 + (P_2)^2 + (P_3)^2\}^{1/2}$ (for fully polarized)

where the degree of polarization (D^p)is defined as:

$$D^P = \{P_1^2 + P_2^2 + P_3^2\} / P_0$$

3.2 Network Nodes along with the E_P Data Key

Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This section concentrates on network nodes which is associated with antagonism along with polarization as strong representatives of their group viewpoints that do not find endorsement from the opposing side. It measures the concentration of high-degree network nodes for each network that have two ranks ř and $ř_b$ where ř is a rank of all network nodes in the sorted measurement, in order of $ř_b$ ranks the nodes, but according to d_p (i.e., number of cross polarization connections) [4]. It uses correlation coefficient ρ to capture the statistical dependence between ř and $ř_b$ that captures the relationship between two variables can be described by a monotonic function and its value ranges from -1 to +1. ρ (X, Y) = 1 means that variable Y is a monotonic function of X. In this context, high ρ (network nodes in low-ranked) indicates concentration of network nodes along with the polarization. A low ρ (network nodes in low-ranked) is in $ř_b$, show significant number of nodes which is not belong to the data key polarization [21].

3.3 Encryption Polarization Vector as Eigenvalue Matrix

In this section, the encryption polarization approach converts the encrypted bits in polarised bits form using the 2x2 matrix [6,8], where eigenvalue matrix is characterized by θ(z) and ϕ(z). These two functions are known polarised vector properties, where E_P can calculated for node network security. The 2x2 matrix represented the polarization state of check bits. Since E_P is based on polarization manipulation, the matrix is very useful. The polarization state of light is described by a 2x1 polarization vector. Any polarization state can be represented as a sum of two perpendicularly polarized check bits with different phase of computation are given in eqn. [1],

$$E_v = \left(xa + yb\, e^{j\delta}\right) E_o\, e^{j\omega t - jkz} \quad \ldots (1)$$

where $|a|^2 + |b|^2 = 1$, and δ is the phase delay between the '**x**' and '**y**' components. The polarised vector corresponding to the check bits are given in eqn. [2],

$$\begin{pmatrix} a \\ be^{j\delta} \end{pmatrix} \quad \ldots (2)$$

It observe that any frequent phase in 'a' and 'b' can be in use and be absorbed by the phase term $e^{j\omega t - jkz}$.

The eigenvalue matrix depends on the definition of the coordinate system. If the coordinate is rotated by ϕ, the matrix also will become different as shown in Figure 8.

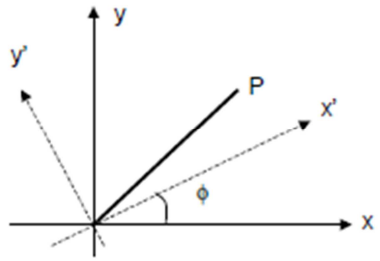


Figure 8: Polarization Rotation by different axis

If the eigenvalue matrix is 'M' in the (x,y) coordinates and M' in the (x',y') coordinate system, then,

$$M' = R_\emptyset\, M\, R_\emptyset^{-1}, \text{ and}$$
$$M = R_\emptyset^{-1}\, M\, R_\emptyset$$

where, R_ϕ is the coordinate transformation matrix,

$$R_\emptyset = \begin{pmatrix} cos\emptyset & sin\emptyset \\ -sin\emptyset & cos\emptyset \end{pmatrix}$$

The eigenvalue matrix of a check bits with position at θ to the different axis as given in eqn. [3],

$$\begin{pmatrix} cos\emptyset & -sin\emptyset \\ sin\emptyset & cos\emptyset \end{pmatrix}\begin{pmatrix} -j & 0 \\ 0 & j \end{pmatrix} \begin{pmatrix} cos\emptyset & sin\emptyset \\ -sin\emptyset & cos\emptyset \end{pmatrix} = \begin{pmatrix} cos2\emptyset & sin2\emptyset \\ sin\emptyset & -cos2\emptyset \end{pmatrix} \quad \ldots (3)$$

After verify the eqn. [3], the conclude polarization matrix is,

$$\begin{pmatrix} cos\emptyset & sin\emptyset \\ -sin\emptyset & cos\emptyset \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} cos2\emptyset \\ sin2\emptyset \end{pmatrix} \quad \ldots (4)$$

which is equivalent to a rotation of the linear polarization along **x** by 2ϕ. This eigenvalue matrix is not the same as the polarization rotation matrix since the rotation is dependent on the polarizer angle for the node network process for data

3.4 Secure Data with Polarization Encryption (E_P)

The proposed polarization encryption (E_P) use bit information of original data to form polarised key. The original data are described by encrypted data formed as linear polarizations [14]. The polarization state at the *(n,k)* component (where, 'n' is number of nodes and 'k' is key generator) is given by a node vector d_{nk}. This polarization is modulated at the *(n,k)* element denoted by a matrix M_{nk}, where assume that each element has two parameters, the direction of the principal axes of E_P for information bits. In this case, M_{nk} is given in eqn. [5] and eqn. [6],

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$M_{nk} = \begin{bmatrix} \exp(-i\lambda_{nk}/2) & 0 \\ 0 & \exp(-i\lambda_{nk}/2) \end{bmatrix} R(\theta_{nk}) \quad \ldots (5)$$

where,

$$R_{nk}(\theta_{nk}) = \begin{bmatrix} cos\ \theta_{nk} & sin\ \theta_{nk} \\ -sin\ \theta_{nk} & cos\ \theta_{nk} \end{bmatrix} \quad \ldots (6)$$

In Eqn. (5) and (6), λ_{jk} and θ_{nk} represent the amount of polarization angle are randomly distributed in the interval [0, 2π]. This variable polarization angle of the principal axes at each node can be realized by combining two clusters in the network. The E_P state e_{nk} is given as eqn. [7],

$$e_{nk} = M_{nk} d_{nk} \quad \ldots (7)$$

Let us suppose that the two input nodes polarization states are,

$$P_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, P_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The modulated node polarization states are calculated from eqn. [5] to eqn. [7] and are given in eqn. [8],

$$e_{nk} = \begin{bmatrix} cos\ \theta_{nk} & \exp\left(-\frac{i\lambda_{nk}}{2}\right) \\ -sin\ \theta_{nk} & \exp\left(\frac{i\lambda_{nk}}{2}\right) \end{bmatrix}$$

$$and \begin{bmatrix} sin\ \theta_{nk} & \exp(-i\lambda_{nk}/2) \\ cos\ \theta_{nk} & \exp(i\lambda_{nk}/2) \end{bmatrix} \quad \ldots (8)$$

for P_1 and P_2, respectively (node polarization states for the network). It shows the e_{nk} can be an arbitrary polarized state by controlling u_{nk} and D_{nk} for P_1 and derive and focus on a node E_P state of e_{nk} are given in eqn. [9] and eqn. [10],

$$e_{nk} = \begin{bmatrix} (e_{nk})_x \\ (e_{nk})_y \end{bmatrix} = \begin{bmatrix} cos\ \theta_{nk} & \exp\left(-\frac{i\lambda_{nk}}{2}\right) \\ -sin\ \theta_{nk} & \exp\left(\frac{i\lambda_{nk}}{2}\right) \end{bmatrix} \quad \ldots (9)$$

$$\frac{[(e_{nk})x]^2}{cos^2\ \theta_{nk}} + \frac{[(e_{nk})y]^2}{sin^2\ \theta_{nk}} + \frac{4\cos\lambda_{nk}}{sin^2\ 2\theta_{nk}}$$

$$(e_{nk})x\ (e_{nk})y = sin^2\lambda_{nk} \quad \ldots (10)$$

Using eqn. [10] obtain the results that the node polarization axes at the (n,k) element with an angle of α_{nk}.

$$\alpha_{nk} = \frac{tan^{-1}(cos\lambda_{nk} tan2\theta_{nk})}{2} \quad \ldots (11)$$

The original E_P at each node can be converted into a random state by the controlling of λ_{nk} and θ_{nk}. Since, the polarization modulation is randomly generated and does not know the original polarization states without information from the encrypted data. When the amount of λ_{nk} and θ_{nk} is larger than π /4, the encryption bit input can be changed with polarization keys. To decrypt the data, a matrix M_{nk}^{-1} that is the inverse matrix of M_{nk} is used and given in eqn. [12].

$$r_{nk} = M_{nk}^{-1}\ e_{nk} = M_{nk}^{-1}\ M_{nk} d_{nk} = d_{nk} \quad \ldots (12)$$

4. NODE PROCESS SECURITY METHODOLOGY

4.1 Encryption and Decryption with Neural Network

In this study, neural network implements the encryption and decryption process between different network nodes and transmit data [9,18] where cycle state capture unit (CSCU) check all bits one-by-one and make sure the trustworthiness of the data between nodes, (refer Figure 9).

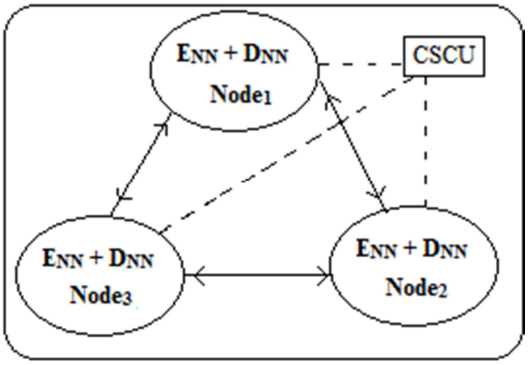


Figure 9: Bit transmission between network nodes

The neural network provides a learning strategy based on parameters optimization to make bits more secure with E_P. A neural network hypothesis space is a continuously parameterized space [12,13] and moreover, the standard loss or error function for a neural network based polarised encrypted bit as given in eqn. [9],

$$L(h(t), d) = (d - h(t))^2 \quad \ldots (9)$$

where, a hypothesis 'h', i.e. the risk associated is given by a bit loss function L() that measures the distance between one bit to another bit as 'd' and h(t).

Figure 10 consist each layer has one or more nodes, where lines between the nodes indicate the flow of information from one node to another node.

Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

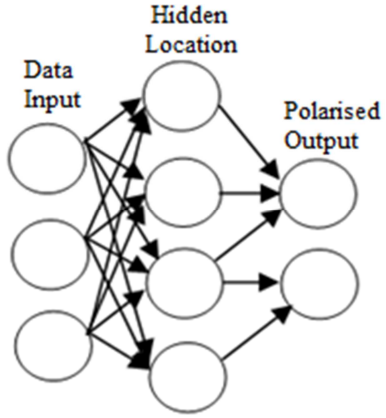


Figure 10: Basics of a neural network for Polarization

The nodes are represented as 'Z' and the information is transmitted via input nodes as 'ZW' and provide output layer, which is represented as active node, shown in Figure 11.

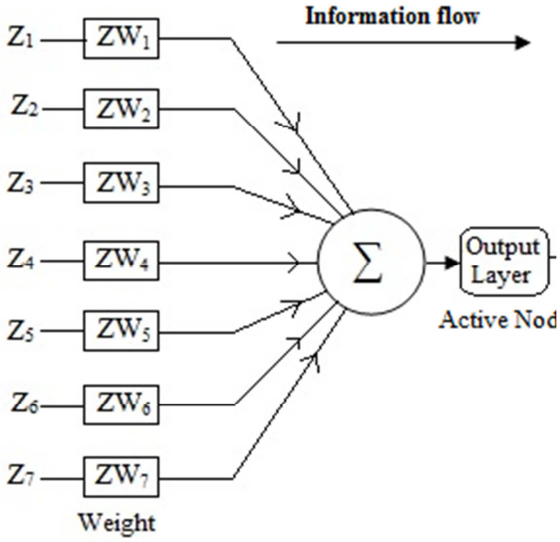


Figure 11: Neural Network Active Node

5. IMPLEMENTATION WORK

***Case 1*:**
Let, b_0 and b_2 be polarised with base zero,
b_1, b_3 and b_4 be polarised with base one

Table 1: Polarized output after checking bits

5-bits (Check bits)					Polarization (Polarized output)				
b4	b3	b2	b1	b0	b4	b3	b2	b1	b0
0	0	0	1	0	1	1	0	0	0
1	0	1	1	0	0	1	1	0	0
0	1	0	0	0	1	0	0	1	0

Note: No need to rotate → 0
Need to rotate → 1
($Rule_1$ → $Node_1$ and $Node_2$ share this information)

The same polarised encryption scheme is used to encrypt the bits received from same cluster of nodes as shown in Figure 12.

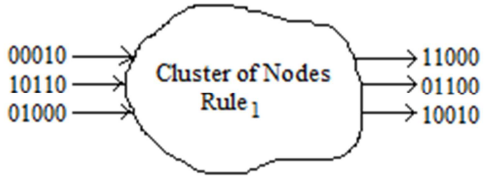


Figure 12: Polarised output for case (i)

***Case 2*:**
Let, b_0 and b_4 be polarised with base zero
b_1, b_2 and b_3 be polarised with base one

Table 2: Polarized output for check bits (with another rule)

5-bits (Check bits)					Polarization (Polarized output)				
b4	b3	b2	b1	b0	b4	b3	b2	b1	b0
0	0	0	1	0	0	1	1	0	0
1	0	1	1	0	1	1	0	0	0
0	1	0	0	0	0	0	1	1	0

The same polarised encryption scheme is used to encrypt the bits received from same cluster of nodes as shown in Figure 13 (for case - 2).

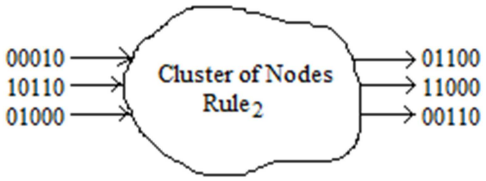


Figure 13: Polarised output for case (ii)

6. FL2440 HARDWARE DEVELOPMENT BOARD

The FL2440 is a development board released by Embedded, is split into two parts,

(i) 6-layer core board and
(ii) 2-layer application board

FL2440 is more flexible and convenience for maintenance. Its layout and wiring are efficiently designed to make more stable and reliable performance and provide BSPs (Board Support Packages) for Embedded Linux and Windows

Journal of Theoretical and Applied Information Technology
20th April 2014. Vol. 62 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

including basic drivers for all the components in the FL2440 Package.

The hardware implementation based python code includes,

(i) Define input–output patterns for training in code
(ii) Create a network with N input, M hidden, and K output nodes using polarised neural network
(iii) The neural network parameters includes,
  (a) The number of input data, hidden location and polarised output nodes
  (b) Creates the weights for input and output nodes using matrix functions
  (c) Input nodes for random values between (-0.2, 0.2) and output nodes for (0.2,-0.2).
  (d) Checks whether the input node is equal to length of inputs, if not then raise an error.

7. RESULTS AND DISCUSSION

Hardware implementation of computation with polarised NN in FL2440 Hardware board using python language. The error plot of conventional and proposed is shown in Figure 14.

Case 1:
Conventional polarised NN without batch weight update (slow convergence)

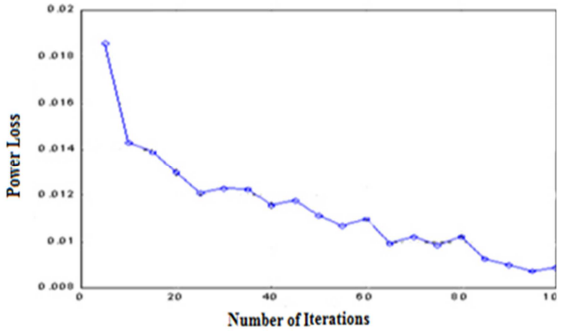
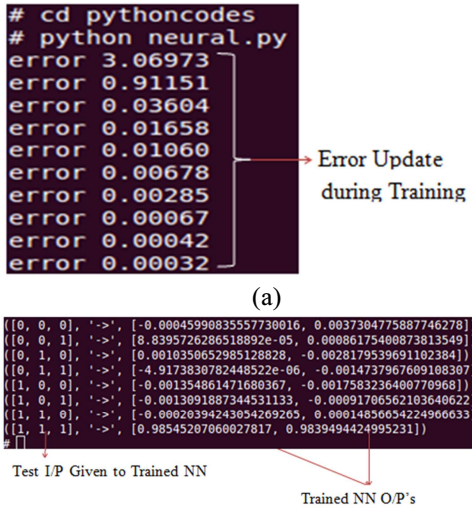


Figure 14: Conventional polarised NN error plot

Case 2:
Proposed polarised NN with batch weight update is shown in Figure 15.



(a)

(b)

Figure 15: (a) Error updation (b) Polarised output with neural network

The hardware output during trainig test output of polarised NN and error plots are shown in Figure 16 to Figure 18.

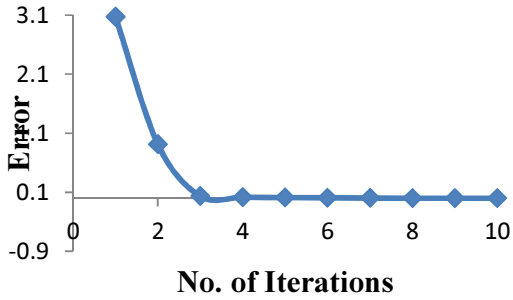
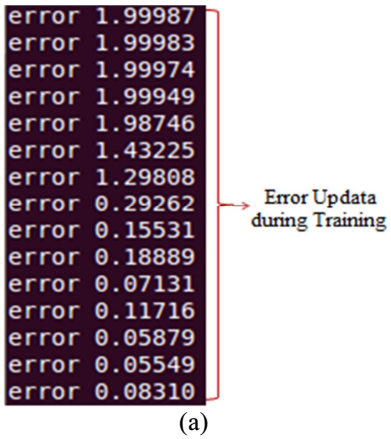
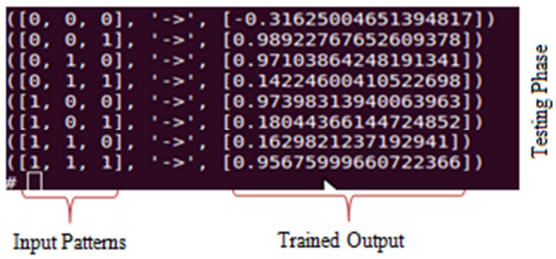


Figure 16: Hardware o/p during Training, Test output of polarised NN and error plot



(a)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(b)

Figure 17: (a) Error updation (b) Polarization output with neural network based encryption

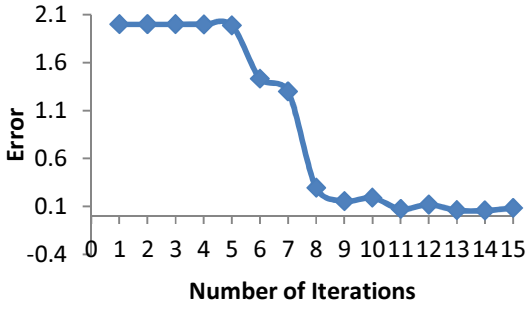


Figure 18: Hardware O/P during Training, Test output of polarised NN and error plot

9. CONCLUSION

In this work, proposed a novel polarized technique using a polarization encryption (E_P) process and represented as a polarization distribution and scrambled by a polarized modulation that can change the polarization state into a random state with neural network for node data security that checks bits position in cluster nodes and make a reliable and secure node data for network users. The polarised output is displayed that when E_P method used python language with polarised NN training, updates an error with every phase of bit and makes better and secure transmission of node data after NN testing phase. In future work, need to work with polarized encryption bits using neutal network to support with huge level network so that all layers also can be used with node network system.

ACKNOWLEDGMENT

I acknowledge the help and facility offered by M/s MicroLogic Systems to carry out the embedded linux and network related studies in hardware environment.

REFERENCES:

[1] Ashwini Galande, Dattatraya Londhe and Mangesh Balpande, "Security in Voip Network Using Neural Network and Encryption Techniques", International Conference on Information and Network Technology, IACSIT Press, Singapore, 2011.

[2] Cagalj M., Capkun S. and Hubaux J.P., "Key agreement in peer-to-peer wireless networks", Proceedings of the IEEE, Special Issue in Security and Cryptography, 94 (2), pp. 467–478, 2006.

[3] Dang-Quan Nguyen and Louise Lamont, "Using Cryptography in Trust Computing for Networked Communications", International Journal of Computer Science (IJCSI), Vol.8, Issue 6, No.1, November 2011.

[4] Davis J. A., McNamara D. E., Cottrell D. M., and Sonhara T., "Two-dimensional **polarization** encoding with a phase-only liquid-crystal spatial light modulator", Application Optics, 39, pp. 1549–1554, 2000.

[5] Deng J., Han R. and Mishra S., "Security support for in network processing in wireless sensor networks", in ACM Workshop on security in Ad Hoc and Sensor Networks (SASN '03), 2003.

[6] Gabriel Biener, Avi Niv, Vladimir Kleiner, Erez Hasman, "Space-variant **polarization** scrambling for image encryption obtained with subwavelength gratings", Science Direct, Optics Communications, 261 pp. 5–12, 2006.

[7] Ganeriwal S. and Srivastava M. B., "Reputation-based Framework for High Integrity Sensor Networks", in ACM Security for Ad-hoc and Sensor Networks (SASN'04), 2004.

[8] Kawano K., T. Ishii, J. Minabe, T. Niitsu, Y. Nishikata and K. Baba, "Holographic recording and retrieval of **polarized** light by use of polyester containing cyanoazobenzen units in the side chain", Optics Lett., 24, pp. 1269–1271, 1999.

[9] Khalil Shihab, "A Backpropagation Neural Network for Computer Network Security", Journal of Computer Science, Science Publications, 2 (9), pp. 710-715, 2006.

[10] Li J., Krohn M., Mazires D. and Shasha, "Secure untrusted data repository (SUNDR)", in Proceeding 6th Symposium, Operating Systems Design and Implementation (OSDI), pp. 121–136, 2004.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[11] Li, C., Li S., Zhang D. and Chen G., "Cryptanalysis of a chaotic neural network based multimedia encryption scheme", Advances in Multimedia Information Processing, PCM, Proceeding, Part III, Lecture Notes in Computer Science., Springer-Verlag, 3333: 418-425, 2004.

[12] Lian S., Sun J. and Wang Z., "Secure Hash function based on neural network", Neurocomputing, Vol.69, No.16-18, 2006.

[13] Manoj Kumar Singh, "Password Based A Generalize Robust Security System Design Using Neural Network", IJCSI International Journal of Computer Science Issues, Vol. 4, No. 2, 2009.

[14] Mogensen P. C. and Gluckstad J., "A phase-based optical encryption system with **polarization** encoding", Optics Communication, 173, pp. 177–183, 2000.

[15] Murugan R. and Shanmugam A., "Cluster Based Node Misbehaviour Detection, Isolation and Authentication Using Threshold Cryptography in Mobile Ad Hoc Networks", International Journal of Computer Science and Security (IJCSS), Vol.6, Issue 3, 2012.

[16] Priyanka Goyal, Sahil Batra and Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International journal of Applications (0975-8887), Vol.9, No.12, November 2010.

[17] Rashid Jalal Qureshi, Khalid Haseeb, Muhammad Arshad, Huma Javed and Haleem Farman, "A Novel Technique Based on Node Registration in MANETs", IJCSI International Journal of Computer Science Issues, Vol.9, Issue 5, No.3, September 2012.

[18] Rudolf Volner and Igor Černák, "Intelligent Communication Networks and Neural Network", European International Journal of Science and Technology, Vol.2 No.6, July 2013.

[19] Srivatsa M. and Liu L., "Vulnerabilities and security threats in structured overlay networks: A quantitative analysis", in proceedings of ACSAC'04, Cambridge, MA, pages 252–261, 2004.

[20] Sunam Ryu, Kevin Butler, Patrick Traynor and Patrick McDaniel, "Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), IEEE Computer Society, 2007.

[21] Vanesa Daza, Javier Herranz, Paz Morillo and Carla Rafols, "Cryptographic techniques for mobile ad-hoc networks", Elsevier, Computer Networks, 51, pp. 4938–4950, 2007.