Innovative Algorithms and Techniques in Automation,
Industrial Electronics and Telecommunications

Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications

Edited by

Tarek Sobh
University of Bridgeport
CT, USA

Khaled Elleithy
University of Bridgeport
CT, USA

Ausif Mahmood
University of Bridgeport
CT, USA

and

Mohammed Karim
Old Dominion University
VA, USA

Springer

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN 978-1-4020-6265-0 (HB)
ISBN 978-1-4020-6266-7 (e-book)

Published by Springer,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

www.springer.com

Printed on acid-free paper

Table of Contents

Preface

This book includes the proceedings of the 2006 International Conference on Telecommunications and Networking (TeNe) and the 2006 International Conference on Industrial Electronics, Technology &Automation (IETA).

TeNe 06 and IETA 06 are part of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 06). The proceedings are a set of rigorously reviewed world-class manuscripts presenting the state of international practice in Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications.

TeNe 06 and IETA 06 are high-caliber research conferences that were conducted online. CISSE 06 received 690 paper submissions and the final program included 370 accepted papers from more than 70 countries, representing the six continents. Each paper received at least two reviews, and authors were required to address review comments prior to presentation and publication.

Conducting TeNe 06 and IETA 06 online presented a number of unique advantages, as follows:

- All communications between the authors, reviewers, and conference organizing committee were done on line, which permitted a short six week period from the paper submission deadline to the beginning of the conference.
- PowerPoint presentations, final paper manuscripts were available to registrants for three weeks prior to the start of the conference
- The conference platform allowed live presentations by several presenters from different locations, with the audio and PowerPoint transmitted to attendees throughout the internet, even on dial up connections. Attendees were able to ask both audio and written questions in a chat room format, and presenters could mark up their slides as they deem fit
- The live audio presentations were also recorded and distributed to participants along with the power points presentations and paper manuscripts within the conference DVD.

The conference organizers are confident that you will find the papers included in this volume interesting and useful.

Tarek M. Sobh, Ph.D., PE
Khaled Elleithy, Ph.D.
Ausif Mahmood, Ph.D.
Mohammed Karim, Ph.D.
Bridgeport, Connecticut
June 2007

Acknowledgements

The 2006 International Conferences on Telecommunications and Networking (TeNe) and Industrial Electronics, Technology & Automation (IETA) and the resulting proceedings could not have been organized without the assistance of a large number of individuals. TeNe and IETA are part of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). CISSE was founded by Professors Tarek Sobh and Khaled Elleithy in 2005, and they set up mechanisms that put it into action. Andrew Rosca wrote the software that allowed conference management, and interaction between the authors and reviewers online. Mr. Tudor Rosca managed the online conference presentation system and was instrumental in ensuring that the event met the highest professional standards. We also want to acknowledge the roles played by Sarosh Patel and Ms. Susan Kristie, our technical and administrative support team.

The technical co-sponsorship provided by the Institute of Electrical and Electronics Engineers (IEEE) and the University of Bridgeport is gratefully appreciated. We would like to express our thanks to Prof. Toshio Fukuda, Chair of the International Advisory Committee and the members of the TeNe and IETA Technical Program Committees including: Abdelshakour Abuzneid, Nirwan Ansari, Hesham El-Sayed, Hakan Ferhatosmanoglu, Ahmed Hambaba, Abdelsalam Helal, Gonhsin Liu, Torleiv Maseng, Anatoly Sachenko, Paul P. Wang, Habib Youssef, Amr El Abbadi, Giua Alessandro, Essam Badreddin, John Billingsley, Angela Di Febbraro, Aydan Erkmen, Navarun Gupta, Junling (Joyce) Hu, Mohamed Kamel, Heba A. Hassan, Heikki N. Koivo, Lawrence Hmurcik, Luu Pham, Saeid Nahavandi, ElSayed Orady, Angel Pobil, Anatoly Sachenko, Sadiq M. Sait, Nariman Sepehri, Bruno Siciliano and Keya Sadeghipour.

The excellent contributions of the authors made this world-class document possible. Each paper received two to four reviews. The reviewers worked tirelessly under a tight schedule and their important work is gratefully appreciated. In particular, we want to acknowledge the contributions of the following individuals: Farid Ahmed, ElSayed Orady, Mariofanna Milanova, Taan Elali, Tarek Taha, Yoichiro Iwasaki, Vijayan Asari, Bruno Siciliano, Navarun Gupta, Mohamed Kamel, Giua Alessandro, Hairong Qi, Abdul Awwal, Seddik Djouadi, Ram Reddy, Anatoly Sachenko, Leon Tolbert, Shuqun Zhang, Mohammad Kaykobad, Vojislav Misic, Sudhir Veerannagari, Osman Tokhi, Mahmoud Mahmoud, Min Song, Mohammad Yeasin, John Billingsley, Alamgir Hossain, Ferdous Alam, Elissa Seidman, Tyler Ross, Fangxing Li, Selim Akl, Anish Anthony, Syed Sajjad Rizvi, Sarhan Musa, Srinivas Manepalli, Hossam Diab, Abdelshakour Abuzneid, Hikmat Farhat,Tingting Meng, Torleiv Maseng, Yenumula Reddy, Zulkefli Yusof, Vojislav

Misic, Hetal Jasani, Hesham El-Sayed, Yu Cai, Casimer DeCusatis, Tyler Ross, Abdelsalam Helal, Muhammad Azizur Rahman, Patricia Gillard, Paul Wang, Mohamed Youssef, Sanjiv Rai, Nirwan Ansari, Munir Majdalawieh, Gonhsin Liu, Ahmed Hambaba, AmirAbdessemed, Kaitung Au, Navarun Gupta, Ram Reddy and Sudhir Veerannagari.

Tarek Sobh, Ph.D., P.E.
Khaled Elleithy, Ph.D.
Ausif Mahmood, Ph.D.
Mohammed Karim, Ph.D.
Bridgeport, Connecticut
June 2007

A Hybrid Predistorter for Nonlinearly Amplified MQAM Signals

Nibaldo Rodríguez A.
University Catholic of Valparaíso of Chile,
Av. Brasil, 2241 nibaldo.rodriguez@ucv.cl

Abstract **– This paper proposes an adaptive baseband Predistortion scheme in order to reduce both nonlinear amplitude and phase distortion introduced by a travelling wave tube amplifier (TWTA) over transmitted 16QAM and 256QAM signals. This compensator is based on a radial basis function neural network (RBF NN) and its coefficients are estimated by using a hybrid algorithm, namely generalised inverse and gradient descent. Computer simulation results confirm that once the 16QAM and 256QAM signals are predistortioned and amplified at an input back off level of 0 dB, there is a reduction of 25 dB and 29 dB spectrum re-growth; respectively. In addition proposed adaptive Predistortion scheme has a low complexity and fast convergence.**

Index Terms – Predistorsion, neural network and multilevel quadratura amplitude modulation.

I. INTRODUCTION

Due to their high spectral and power efficiency, multilevel quadrature amplitude modulation (MQAM) is a technique widely used in commercial communications systems, such as digital video broadcasting satellite and terrestrial standards [1,2]. However, MQAM shows a great sensibility to the non-linear distortion introduced by the travelling wave tube amplifier (TWTA), due to fluctuations of its non-constant envelope. Typically, a TWTA is modulated by non-lineal amplitude modulation to amplitude modulation (AM-AM) and phase to modulation (AM-PM) functions in either polar or quadrature form [3]. To reduce both AM-AM and AM-PM distortions, it is necessary to operate the TWTA with a large power back off level, but these operations reduce the TWTA's output power. During the last year, other solutions have been proposed to reduce both AM-AM and AM-MP distortion by using Predistortion (PD) based on polynomial model [4-7], Volterra serie [8-10] and neural network [11-16]. This paper only deals with the neural network model, due to its capacity of approximating to different non-lineal functions. The predistorters have been reported in references [11-16] to use two neural networks for compensating both nonlinear amplitude and phase distortion. The disadvantage of these neural network predistortion techniques is their slow convergence speed, due to the classical back-propagation algorithm, and also to the ignorance of the early data. However, our predistortion scheme only uses one radial basis function neural network for compensating both nonlinear AM-AM and AM-PM distortions introduced by TWTA, which permits to reduce computer storage requirements, and to increase the predistorter coefficients adaptation speed.

The aim of the proposed radial basis function neural network predistorter is to reduce both nonlinear amplitude and phase distortion introduced by TWTA over transmitted 16QAM and 256QAM signals. The predistorter structure is based on a radial basis function neural network and its coefficients are found by using a hybrid algorithm, which combined gradient-descent method with Moore-Penrose generalized inverse [17].

The remainder of this paper is organized as follows: In section II, it is presented a systems description of the proposed scheme. The linearisation technique of the TWTA, and hybrid learning algorithm for adjusting the neuronal predistorter coefficients are presented in Section III. The performance curves of the spectrum regrowth and signal constellation warping effect of the 16QAM and 256QAM signals are discussed in Section IV. Finally, the conclusions are presented in the last section.

II. SYSTEM DESCRIPTION

The input data bits are encoded by using the M-QAM mapper device, which maps a k-tuple of bits over MQAM ($M=2^k$) symbols by using Gray coding. The transmitter filter is implemented as a square root raised cosine (SRRC) pulse shaping distributed at the transmitter and receiver with L-taps, roll-off parameter β and over-sample factor of 8 samples per symbol. The modulated baseband signal $x(t)$ is first pre-distorted and nonlinearly amplified, then propagated over an additive white Gaussian noise (AWGN) channel. The signal amplified is represented by:

$$z(t) = A(|y(t)|)\exp[j\cdot\{\angle y(t) + \Phi(|y(t)|)\}] \tag{1}$$

where $|y(t)|$ and $\angle y(t)$ are the amplitude and phase of the predistorted complex signal $y(t)$. The function $A(\cdot)$ and $\Phi(\cdot)$ denote AM-AM conversion (nonlinear amplitude) and AM-PM conversion (nonlinear phase); respectively.
For a TWTA, the expressions for $A(\cdot)$ and $\Phi(\cdot)$ are given by [3] as:

$$A(|y(t)|) = \frac{\alpha_A |y(t)|}{1+\beta_A |y(t)|^2} \tag{2}$$

$$\Phi(|y(t)|) = \frac{\alpha_\Phi |y(t)|^2}{1+\beta_\Phi |y(t)|^2} \tag{3}$$

with $\alpha_A = 2$, $\beta_A = 1$, $\alpha_\Phi = \pi/3$ and $\beta_\Phi = 1$.
The nonlinear distortion of a high power amplifier depends on the back off. The input back off (IBO) power is defined as the ratio of the saturation input power, where the output power begins to saturate, to the average input power:

$$IBO = 10\log_{10}\left(\frac{P_{i,sat}}{P_{i,avg}}\right) \tag{4}$$

where $P_{i,sat}$ is the saturation input power and $P_{i,avg}$ is the average power at the input of the TWTA.
At time t, the received signal $r(t)$ is defined by

$$r(t) = z(t) + n(t) \tag{5}$$

T. Sobh et al. (eds.), Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, 1–4.

where $n(t)$ represent the complex AWGN with two-sided spectral density $N_0/2$.

The received signal $r(t)$ is passed through the matched filter (SRRC), and then sampled at the symbol rate $1/T$. The sequence at the output of the sampler p_k is fed to the MQAM Demapper. The Demapper splits the complex symbols into quadrature and in-phase components, and puts them into a decision device, where they are demodulated independently against their respective decision boundaries. Finally, output bits stream $\hat{d}_k$ are estimated.

III. HYBRID PREDISTORTION ALGORITHM

Consider the input signal $x(t)$ with polar represention given by:

$$x(t) = r_x(t)\exp\left[j\theta_x(t)\right] \tag{6}$$

where r_x and θ_x represent the modulated envelope and the phase; respectively.

The output of the PD is then given by:

$$y(t) = M\left[r_x(t)\right]\exp\left[j\left\{\theta_x(t) + N\left(r_x(t)\right)\right\}\right] \tag{7}$$

Now, using equation (1) and equation (7) we obtain complex signal envelope at the TWTA output as:

$$z(t) = A\left[M\left(r_x(t)\right)\right]\exp\left[j\left\{\theta_x(t) + N\left(r_x(t)\right)+\right\}\right]\cdot \exp\left[j\Phi\left[M\left(r_x(t)\right)\right]\right] \tag{8}$$

In order to achieve the ideal predistortion function, the signal $z(t)$ will be equivalent to the input signal $x(t)$. That is:

$$M\left[r_x(t)\right] = A^{-1}\left[r_x(t)\right] \tag{9}$$

where $A(.)^{-1}$ represents inverse amplitude function of the TWTA and:

$$N\left[r_x(t)\right] = -\Phi\left[A^{-1}\left(r_x(t)\right)\right] \tag{10}$$

where $N(.)$ represents inverse phase function of the TWTA.

Therefore, ideal predistorted output $y(t)$ is obtained as:

$$y(t) = A^{-1}\left[r_x(t)\right]\exp\left\{j\left[\theta_x(t) - \Phi\left(A^{-1}\left[r_x(t)\right]\right)\right]\right\} \tag{11}$$

Finally, in order to achieve the ideal predistortion function $f_{PD}(.) = y(t)$, it is only necessary to find the real-valued function $A^{-1}(.)$. To approximate the function $A^{-1}(.)$, a radial basis function neural network is used and the weights are determined from a finite number of samples of the function $A(.)$.

During the training process, the signal $x(t)$ is equal to the signal $y(t)$, but during decision-direct mode the signal $y(t)$ will be the desired predistorted signal. The training process was done by using the trial and error method. In order to implement the training process, it is necessary to obtain a database Γ containing the output amplitude $r_z(n)$ of the TWTA, and the corresponding desired output $r_x(n)$, $\Gamma = \{r_z(n), r_x(n);\ n = 1,...,N_s\}$, where the N_s value represents the sample number of the function $A(.)$, and the desired output r_x is obtained as:

$$r_x(n) = \frac{|x(n)|}{\max\left\{|x(n)|\right\}}\cdot IBO \tag{12}$$

The output of the PD is obtained as:

$$\begin{aligned} &\hat{y}_k = \sum_{j=0}^{N_c} w_j H_{jk}, \quad k = 1,2,...,N_s \\ &H_{jk} = \Psi(u), \quad H_{0k} = 1 \\ &u = \left\|\left(|z_k| - c_j\right)\right\|^2 \\ &\Psi(u) = u + 1 \end{aligned} \tag{13}$$

where the N_c value represents the number of centre in the hidden layer. The weights $\{w_j, c_j\}$ represent the interconnections of the hidden and output layer, respectively, and $\Psi(.)$ denoted the non-linear activation function of the hidden centres.

The goal of the learning algorithm is to find the weights vector that minimizes the cost function defined by:

$$\begin{aligned} E\left[r_z(n), c, w\right] &= \frac{1}{N_s}\sum_{n=1}^{N_s} e^2(n) \\ &= \frac{1}{N_s}\sum_{n=1}^{N_s}\left[Gr_x(n) - \hat{y}\left(r_z(n), c, w\right)\right]^2 \end{aligned} \tag{14}$$

where $Gr_x(n)$ represents desired linear model, and G depends on Peak Back off (PBO) of the TWTA, which denotes the difference between saturation power P_s and the maximum desired output power of the linearised TWTA, SP_s. The PBO is obtained as:

$$\begin{aligned} &PBO = -10\log_{10}(S) \\ &S = \frac{G}{P_s}, \quad 0 < S \le 1 \end{aligned} \tag{15}$$

The PD parameters are estimates by using a hybrid algorithm based on both the Moore-Penrose generalised inverse and gradient descent method.

Assuming the c_j weights in the previous iterations are known, we can derive the generalised inverse solution as:

$$\hat{w} = \left(H^T H\right)^{-1} H^T |Gx| \tag{16}$$

Once w_j are obtained, gradient descent method can be used to update the c_j weights. Then the new c_j weights are found as:

$$c = c - \mu\frac{\partial E}{\partial c} \tag{17}$$

Where μ represent learning rate and $\partial E/\partial c$ is gradient vector of E with the jth element of the vector c and the gradient vector of E is given by:

$$\frac{\partial E}{\partial c_j} = \sum_{k=1}^{N_s} 2\Psi' \left[\left\| \left(|z_k| - c_j \right) \right\|^2 \right] \left(|z_k| - c_j \right) \left(|Gx_k| - \hat{y}_k \right) \hat{w}_j \qquad (18)$$

IV. SIMUALATION RESULTS

In this section, it is presented the performance evaluation of the nonlinear distortion compensation scheme. The signals are filtered with 81-tap SRRC pulse shaping for the power spectral density (PSD) calculation and with 47-tap SRRC pulse shaping for the constellation. In addition, in all calculations the pulse shaping filter was implemented with a roll-off factor of $\beta = 0.35$ and 8 samples per symbol.

The parameters of the neural predistorter were estimated during the training process using $N_s = 100$ samples of the amplitude $A(.)$ for 16QAM signals, and the TWTA was operated with IBO of -0.5 dB and a power PBO of -0.22 dB. The neural predistorter was configured with one input node, one linear output node, four nonlinear hidden centres and one bias unit for hidden layer; respectively. In the training process the initial weights, $c(0)$, were initialised by a Gaussian random process with a normal distribution $N(0,1)$. The training process was run with 3 trials and the normalised mean square error (NMSE) after convergence was approximately equal to -50 dB.

In decision-direct mode, the neural predistorter is simply a copy of the neural network obtained in training process.

Figure 1, show the power spectral density (PSD) curves of multilevel quadrature amplitude modulation schemes for both linearly and nonlinearly amplified 16QAM and 256QAM signals. In one hand, for the nonlinear amplification case only with TWTA, the PSD curves are denoted as 16QAM TWTA and 256QAM TWTA; respectively. By the other hand, for the nonlinear amplification case with predistortion and TWTA, the curves are denoted as 16QAM PD TWTA and 256QAM PD TWTA. It can be seen that 16QAM TWTA and 256QAM TWTA have a degradation of PSD about 25 dB and 29dB; respectively. Moreover, from the figure can be seen that the curves of spectral re-growth of the nonlinear case with predistortion are very close to the linear case due to the incorporation of the proposed neural predistorter. Therefore, the proposed predistortion schemes allow to reduce significantly the degradation of the spectral re-growth for 16QAM and 256QAM signals at an IBO level of 0 dB.

The effects of nonlinearity on the received 256QAM constellations in the absence of the channel AWGN are shown in Figure 2 and 3, which correspond to the TWTA without and with predistortion scheme operated at an input back off level of 0 dB. According to Figures 2, it is observed that square 256QAM constellation is severely distorted by the nonlinear AM-AM and AM-PM characteristics of the TWTA without predistortion. This distortion is interpreted as noise in-band, and it is called constellation warping effect. According to Figures 3, the proposed predistorter reduces significantly the constellation warping effect on received 256QAM signals.

Therefore, comparing Figures 2 and 3, it can be seen that constellation warping effect is reduced significantly by using proposed predistoter. Moreover, it permits to reduce both computer storage requirements and coefficients adaptation time of the predistorter, which is achieved due to the proposed hybrid algorithm; it only uses one radial basis function neural network for compensating both nonlinear AM-AM and AM-PM characteristics of the TWTA.

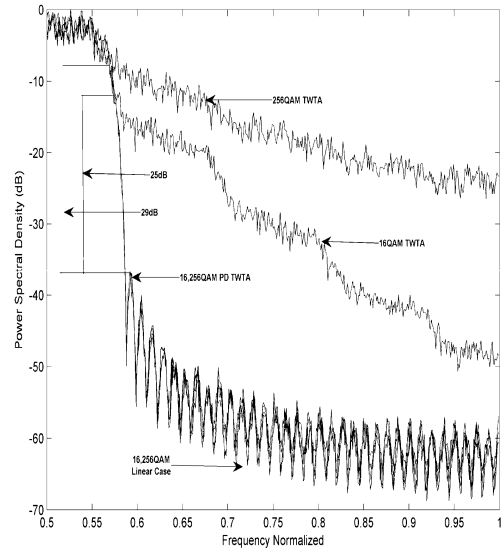

Figure 1 Power spectral densities of 16QAM and 256QAM signals with and without predistortion at IBO= 0 dB.

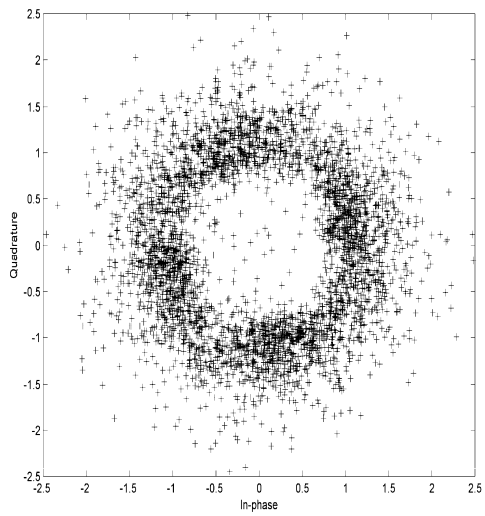

Figure 2 Constellation warping effect over received 256QAM signal due to TWTA with IBO= 0 dB

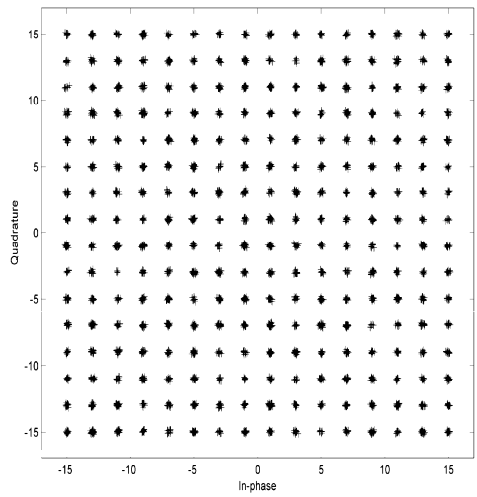

Figure 3 Constellation warping effect over received 256QAM signal compensate with predistortion at IBO= 0 dB

V. CONCLUSIONS

An adaptive baseband predistortion scheme based on a radial basis function neural network for linearising a TWTA has been presented in this paper. The proposed predistorter uses only a neural network with nine coefficients to compensate non-lineal amplitude and phase distortion introduced by the TWTA over transmitted 16QAM and 256QAM signals. The predistorter coefficients adaptation was found by using 3 iterations of a hybrid algorithm based on both generalised inverse and gradient descent method. Simulation results have shown that the proposed predistortion scheme can prevent the RF transmitter from spectrum re-growth and constellation warping effect due to TWTA's nonlinearity with a low complexity and fast convergence.

REFERENCES

[1] ETSI, *Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 GHz Satellite Services*, EN 300 421 v.1.1.2, August 1997.

[2] ETSI, *Digital Video Broadcasting (DVB): Framing structure, channel coding and modulation for digital terrestrial television*, EN 300 744, August 1997.

[3] A. M. Saleh, *Frecuency-Independent and Frecuency-Dependent nolinear models TWT amplifiers*, IEEE Trans. Comm., Vol. COM-29, pp. 1715-1719, November 1981.

[4] R. Raich, H. Qian, and G. T. Zhou, *Orthogonal polynomials for power amplifier modeling and predistorter design*, IEEE Trans. on Vehicular Technology, Vol. 53, Nº. 5, pp. 1468-1479, September 2004.

[5] L. Ding and G. T. Zhou, *Effects of even-order nonlinear terms on power amplifier modeling and predistortion linearization*, IEEE Trans. on Vehicular Technology, Vol. 53, Nº. 1, pp. 156-162, January 2004.

[6] R. Marsalek, P. Jardin and G. Baudoin, *From post-distortion to pre-distortion for power amplifier linearization*, IEEE Comm. Letters, Vol. 7, Nº7, pp.308-310,July,2003.

[7] M. Ghaderi, S. Kumar and D.E. Dodds, *Fast adaptive polynomial I and Q predistorter with global optimisation*, IEE Proc-Comm., Vol. 143, Nº. 2, pp. 78-86, April 1996.

[8] L. Ding, R. Raich, and G.T. Zhou, *A Hammerstein predistortion linearization design based on the indirect learning architecture*, Proc. Int. Conference on Acoustics, Speech, and Signal Processing (ICASSP'2002), Vol. 3, pp. 2689-2692, Orlando, FL, May 2002.

[9] M. Ibnkahla, *Natural gradient learning neural networks for adaptive inversion of Hammerstein systems*, IEEE Signal Processing Letters, pp. 315-317, October 2002

[10] C. Eun and E. J. Power, *A new Volterra predistorter based on the indirect learning architecture*, IEEE Trans. Signal Processing, Vol. 45, pp. 223-227, January 1997

[11] D. Hong-min., H. Song-bai and Y. Jue-bang, *An adaptive predistorter using modified neural networks combined with a fuzzy controller for nonlinear power amplifiers*, Int. Journal of RF and Microwave Computer-Aided Engineering, Vol. 14, Nº 1, pp. 15-20, December, 2003

[12] N. Rodriguez, I. Soto and R. A. Carrasco, *Adaptive predistortion of COFDM signals for a mobile satellite channel*, Int. Journal of Comm. Systems, vol. 16, Nº 2, pp. 137-150, February, 2003.

[13] F. Abdulkader, Langket, D. Roviras and F. Castanie, *Natural gradient algorithm for neural networks applied to non-linear high power amplifiers*, Int. Journal of Adaptive Control and Signal Processing, Vol. 16, pp. 557-576, 2002

[14] M. Ibnkahla, *Neural network modelling predistortion technique for digital satellite communications*, in Proc. IEEE ICASSP, Vol. 6, pp. 3506-3509, 2000.

[15] M. Ibnkahla, J. Sombrin J., F. Castanié and N.J. Bershad, *Neural network for modeling non-linear memoryless communications channels*, IEEE Trans. Comm. Nº 45 (7), pp. 768-771, July 1997.

[16] B.E. Watkins and R. North, *Predistortion of nonlinear amplifier using neural networks*, in Proc. IEEE Military communications Conf., Vol.1, pp. 316-320, 1996

[17] D. Serre, Matrices: Theory and applications. New York: Springer-Verlag, 2002

Safe Logon with Free Lightweight Technologies

S. Encheva
Stord/Haugesund University College
Department Haugesund
Bjørnsonsg. 45, 5528 Haugesund
Norway

S. Tumin
University of Bergen
IT Department
P.O.Box 7800, 5020 Bergen
Norway

***Abstract*—In this paper we address some security problems and issues about implementing Web applications and Web services. In order to do this, we first identify trust relationships among users and systems. In particular, we look into the problems of a secure communication between two parties over insecure channels using a signed digital envelope. We propose a simple and secure way of sign-on into Web applications without using enterprise user-identification and password pair. We try to adhere to simplicity principle in our modeling of the system. By using simple model and free lightweight technologies, we show that it is possible to implement secure Web applications and services.**

I. INTRODUCTION

Security within information systems context is based on a complicated trust relations and questions on communication prospective. Trust relations are established between two communicating parties in a relation such as sender/receiver and client/server. When such relations cannot establish trust directly, trusted third parties are used as mediators, which can complicate matters even farther. Security is taken differently by different persons with different prospective of the communicating systems. To a user, security might mean protection on privacy, identity theft and against framing. To an administrator, responsible for the correct working of the applications, security might mean protection on data and process integrity, information flow and recourses protection. The (user, application) pair leads to the necessary establishment of four trust relations among them; application-application, user-application, application-user and user-user. In practice these trust relations are made mutual by, 'I trust you if you trust me' principle. For example, an application trusts a user if the user provides a valid credential at sign-on, the user in turn trusts the application to protect its data and process such that, his/her identity has not being compromised. Whose fault is it when an identity is caught doing an illegal act? Is it a dishonest user, who is the owner of the identity, or an application with weak security policies and implementation, which allow identities theft to occur? It might well be the fault of a weak communication link protocol which leak users' identity under the establishment of trust relations mention above.

In this paper we propose some security tools based on open-source software for Web applications/services for teams of developers and implementers of limited size. Web applications/services have been developed and deployed due to necessity and not based on commercial goals.

Members of development teams (developers and engineers), normally have different levels of technical knowledge, experience and know-how. Usually, such a project concentrates on workability of a system in a complex environment rather than producing commercial grade software for an assumed environment. To meet the workability goal, security concerns are not taken into consideration due to lack of experience and/or work knowledge. We believe that by using simple and open-ended software tools, developers, and implementers can achieve both workability and a higher level of security due to the fact that a system being developed is under a full control of the developers.

The paper is organized as follows. Related work is presented in Section 2. Trust relations are discussed in Section 3. In Section 4 we proposed the use of signed massage of digital envelope package to be used in XML-RPC communication that ensures security, privacy and non-repudiation. A method of using password card called PASS-card for Web sign-on that does not disclose users' system credentials is presented in Section 5. The paper ends with a conclusion.

II. RELATED WORK

Network security problems are discussed in [1]. A set of hints for designing a secure client authentication scheme is described in [4]. A taxonomy of single sign-on systems is presented in [9].

XML-RPC [8] is a Remote Procedure Calling protocol that works over the Internet. An XML-RPC message is an HTTP-POST request. The body of the request is in XML. A procedure executes on the server and the value it returns is also formatted in XML. Procedure parameters can be scalars, numbers, strings, dates, etc., and can also be complex record and list structures.

PGPi is the international variant of Pretty Good Privacy (PGP) [7], which provides an email encryption system. PGP is normally used to apply digital signatures to emails and can also encrypt emails, and thus provides privacy.

T. Sobh et al. (eds.), Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, 5–9.

A public key encryption program was originally written in 1991. Later PGP versions have been developed and distributed by MIT, ViaCrypt, PGP Inc., and Network Associates Inc. (NAI). PGP is used as a standard for email encryption today, with millions of users worldwide.

PGP does not depend on the traditional hierarchical trust architecture but rather adopts the 'web of trust' approach [10]. Trust issues related to network are discussed by [5].

Limitations to existing e-commerce technologies: data resides in traditional databases, and security is difficult to guarantee across network [2]. Practical sides of Public Key Infrastructure (PKI) are presented in [3].

III. TRUST RELATIONS

Application-Application

Here the sender and the receiver are communicating programs across an insecure channel. A message can be a data synchronization job using push or pull mechanism, a remote procedure request and response, or an even reported by a software agent. The message can be stored and copied. The message needs to be protected against disclosure and tempering on route.

User-Application

Users' credentials and authorization data are protected by a secure sign-on service. When a user gives his/her credentials or other sensitive information to an application, he/she needs to be sure that these data really go to the intended server and are not copied and forwarded to another programs.

Application-User

The user-management system must provide users with strong password policies and a framework where applications will not be compromised by weak users' passwords and weak authentication and authorization mechanism.

User-User

The sender and the receiver agree on a non-refutable mutual contract on the originality and validity of the messages passed between them.

IV. DIGITAL ENVELOPE

In our framework, the sender (Fig. 1), encrypts a message (*payload*) by a symmetric cryptographic function (*sc_crypto*) using a secret-key (*skey*) to produce encrypted payload (*A)*.

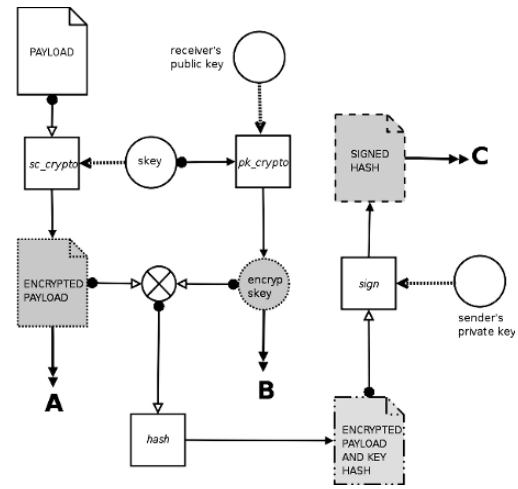

Fig. 1. Sender

A public-key cryptography function (*pk_crypto*) is used to encrypt the secret-key (*B*) using the public-key of the receiving party. Symmetric cryptographic (for example Blowfish) functions for encryption and decryption using a secret key are faster and less resources (CPU, memory) intensive then the public-key cryptography. Together, they (*A* and *B*) make a message in a digital envelope.

The sender takes the digital envelope and runs it through a hash function (*hash)* to produce a hash value. A one-way hash function generates a unique text string to the given input. The hash value is then encrypted by public-key cryptography function (*sign*) using the sender's private key to create a digital signature (*signed hash*) and this authenticates the sender, since only the owner of that private key could encrypt the message.

The *A*, *B* and *C* components are then packed together into a request package. On message arrival, the receiver unpacks the request package back into *A*, *B* and *C* and does the reverse process of decryption and verification (Fig. 2).

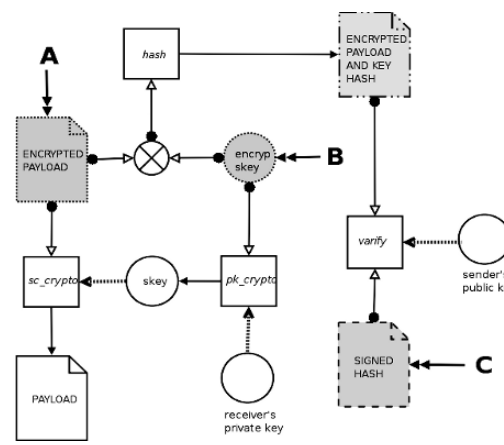

Fig. 2. Receiver

For *Application-Application* communication based on an XML-RPC (XML based remote procedure call over HTTP) request, the receiver unpacks the *payload* to get the procedure name and its parameters. On XML-RPC response, the receiver unpacks the *payload* to get return values. Actually, the payload data is a data structure made into XML by using a Python's xmlrpclib module.

For XML-RPC messages, the *skeys* used are made different for different messages. The requester signs its request message and the responder signs its response message.

Most User-User communications are based on email. Users exchange messages using SMTP (Simple Mail Transfer Protocol). Sadly, it is easy to spoof email (forge email sender) because SMTP (Simple Mail Transfer Protocol) lacks authentication. With a wrong configuration of a mail server which allows unrestrictive connections to the SMTP port will let anyone from anywhere to connect to the SMTP port of the site and send email with a forged email sender.

By email spoofing, a user receives email that appears to have originated from one sender when it actually was sent from another sender. Email spoofing is often an attempt to frame another user of making a damaging statement. By claiming to be from a system administrator, a user is tricked into releasing sensitive information (such as passwords).

Users can exchange authenticated email messages by using cryptographic signatures, for example PGP. Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit. However, PGP does not provide privacy since the messages are not encrypted in any way.

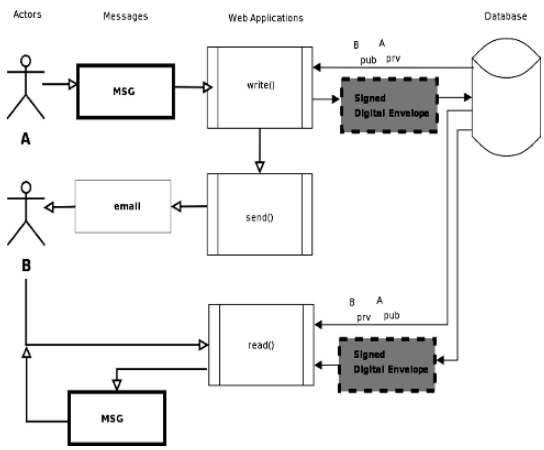

Fig. 3. User-User

Signed digital envelope mechanism can be used in a Web application for User-User communication that ensures secure and non-refutable exchange of messages. In a simple implementation, both the private and public keys of the user are stored in a secure database by the application. The private keys are protected by users' passwords. After a valid sign-on, the writer uploads his/her message. The application will then ask a list of recipients of this message. Each message to each recipient will then be made into a digital envelope using public key of the recipient. Each of these digital envelopes is then signed using the writer's private key.

These messages packed in signed digital envelopes are then saved in the database ready to be read by the recipients. The application will then send an email to each recipient about the message and on how to read it. A recipient can follow the hyper-link provided in the email to read the message. The recipient is sure that the message is written by the writer if the verify process using the writer's public key is successful. By using the recipient's private key, the recipient can extract the secret-key used to encrypt message. Using this secret-key the recipient can then decrypt the encrypted message in order to read it.

V. THE PASS CARD

Consider the environment in which a user is connected to a Web application. A user can run a Web browser on any PC, some of which are situated in public rooms. The user can not be sure that the PC is secure and free from spy-wares.

A single credential policy increases the risk of the system wide security breach, should that credential got stolen. A keyboard grabber program can easily steal users' credentials without user's knowledge. One solution is not to use a {user-identification, password}-pair credentials for Web applications' sign-on. Some of the technologies supporting such a solution are the use of Smart-cards, biometric devices, and a {client certificate, pin}-pair method.

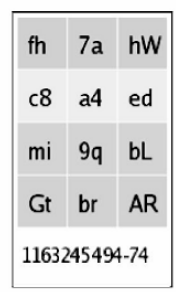

Fig. 4. PASS-Card

We propose a method of using a password card called PASS-card for Web sign-on that does not disclose users' system credentials. A user can produce a PASS-card (a randomly generated image, similar to Fig. 4) via a Web application from a PC within a trusted network, like for example organization's internal network, at anytime. A user has to choose a nick-name and a PIN-code while producing a PASS-card. A PASS-card contains twelve couples and a serial number (Fig. 4). Each couple consists of two randomly generated characters.

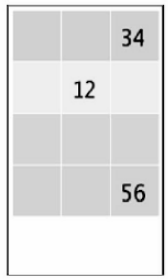

Fig. 5. KEY-map

During any process of sign-on, the system will present to the users with KEY-map diagrams similar to the one on Fig. 5 as a part of the sign-on process. The sign-on application randomly picks and places three couples on the KEY-map locations.

These three couples are randomly positioned in the KEY-map diagram to form a PASS key for this particular sign-on session, Fig. 6.

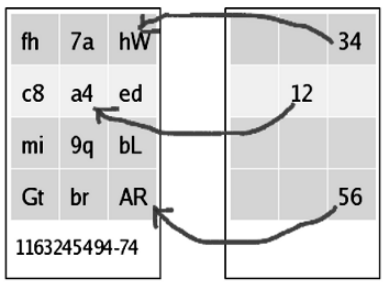

Fig. 6. PASS Keys

To sign-on the user must provide the correct PASS-key correspond to the given KEY-map (the right-hand side figure in Fig. 6). For this particular example (Fig. 6), the PASS key contains three pairs: the first pair (12) which corresponds to the couple *a4* , the second pair (34) which corresponds to the couple *hW* and the third pair (56) which corresponds to the couple *AR*. The resulting sequence *a4hWAR* is the user's PASS-key for this particular sign-on process.

The KEY-map diagram is an image file randomly generated by the Web application using the Python's GD module for each sign-on. PASS-card and KEY-map provide system's users with changing six characters password for each new sign-on.

The user proves his/her authenticity to the application by giving a correct PASS-key from the PASS-card mapped by the KEY-map, the correct nick-name connected to his/her PASS-card and the correct PIN-code. The system then proves its validity by presenting the user with the PASS-card serial number. The valid triplet {PASS-key, nick-name, PIN-code} is then mapped to the real system user.

A user can revoke his/her PASS-card from anywhere and obtain a new one within a trusted network at anytime.

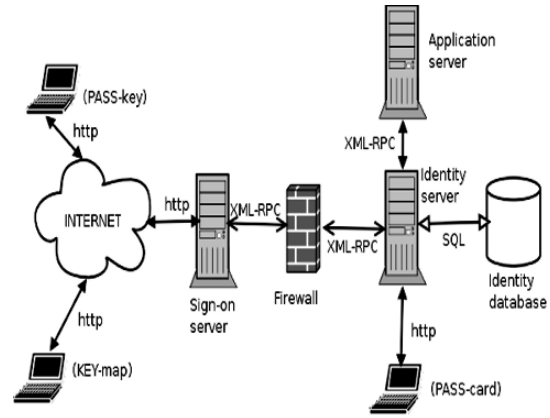

Fig. 7. PASS-Card sign-on

The system architecture that supports PASS-card is shown in Fig. 7. The XML-RPC traffics are made secure by sending messages in signed digital envelopes.

VI. CONCLUSION

In this paper we have identified trust relationships among users and applications. These trust relationships can be broken by undesirable events made possible due to insecure communication environment between two communicating parties. We propose several security tools that can be used to increase the security on the communication channels, thus also increase the trust level.

We adhere to simplicity principle in our modeling of the system. By using simple model and free lightweight technologies, we show that it is possible to implement secure Web application/services. All the applications mentioned in this paper are written in Python scripting language and are making use of Python modules.

XML-RPC with signed digital envelope makes it possible to transmit request/response messages trustworthy, securely and privately over an insecure public network. Users can write private and non-refutable messages to each other using signed digital envelope. A secure User-User messaging system based on signed digital envelope, in which messages between application's users are made private and trustworthy, was proposed.

The use of public-key cryptography introduces the problem of public-key management. The management of users' identities and public-keys is not a trivial matter. The security of private-keys is the essential part of the public-key cryptography.

User authentication based on user-identification and password for sign-on to Web based applications can break the security of the entire enterprise. We proposed a sign-on mechanism using PASS-cards. We use Apache Web server with mod_python to implement the system shown in Fig. 7. PASS-cards allow the user to sign-on from virtually anywhere (by using only http) without

fear of disclosing his/her real system credential. The users themselves administer the usage and validity the PASS-cards they owned.

REFERENCES

[1] J. Albanese, J, and W. Sonnenreich, 2003, "Network Security Illustrated," *McGraw-Hill Professional*, 2003.

[2] S. Garfinkel, "Web Security, Privacy and Commerce," *O'Reilly*, 2002.

[3] E. Geschwinde, and H.-J. Schonig, "PostgreSQL, Developer's Hadbook," *Sams Publishing*, USA, 2001.

[4] K. Fu, E. Sit, K. Smith, and N. Feamster, "Dos and Don'ts of Client Authentication on the Web," *10th USENIX Security Symposium*, Washington, D.C, 2001.

[5] Y. Lu, W. Wang, D. Xu, and B. Bhargava, "Trust-based Privacy Preservation for Peer-to-peer Data Sharing," *Proceedings of the 1st NSF/NSA/AFRL workshop on Secure Knowledge Management (SKM)*, 2004.

[6] http://www.pubcookie.org

[7] http://www.pgpi.org

[8] http://www.xmlrpc.com/

[9] A. Pashalidis, and C. J Mitchell, "A taxonomy of single sign-on Systems," *Lecture Notes in Computer Science*, vol. 2727, pp.249-264, 2003.

[10] P. Zimmermann, "Pretty Good Privacy User's Guide," *Distributed with the PGP software*, 1993.

Stochastic Communication in Application Specific Networks–on–Chip

Vivek Kumar Sehgal[1] and Nitin[2]
[1]Department of ECE and [2]Department of CSE & IT
Jaypee University of Information Technology
Waknaghat, Solan–173215, HP, INDIA
{vivekseh, er.nitin}@gmail.com

***Abstract*- Networks-on-chip (NoC) is a new approach to System-on-chip (SoC) design. NoC consists of different Intellectual Property (IP) cores. The NoC solution brings a networking method to on-chip communication and claims roughly a threefold increase in performance over conventional bus systems. In this paper we proposed a new method for stochastic communication between the different IP cores. These IP cores are connected with different routers or switches and are treated as different compartments on the single chip. The spread of information among these IP cores can be represent using a closed donor control based compartmental model, which can be converted into a stochastic model. The stochastic model is more realistic and enables us to compute the transition probability from one IP to other IP core as well as latency.**

I. INTRODUCTION

System-on-chip (SoC) designs provide integrated solutions to challenging design problems in the telecommunications, multimedia, and consumer electronic domains. With deep sub-micron technology, chip designers are expected to create SoC solutions by connecting different Intellectual Property (IP) cores using efficient and reliable interconnection schemes known as Networks-on-Chip (NoC). This methodology makes a clear distinction between computation (the tasks performed by the IP cores) and communication (the interconnecting architecture between the IP cores). NoC are formed by connecting either homogeneous or heterogeneous IP cores on a single chip. Since modern NoC are becoming extremely complex, so there are many challenges in this new area of research. On-chip wire delays have become more critical than gate delays and recently synchronization problems between Intellectual Properties (IPs) are more apparent. This trend only worsens as the clock frequencies increase and the feature sizes decrease [1]. However, low latency which is an important factor in real time applications [2].The interconnects on chip are subject to new types of malfunctions and failures that are harder to predict and avoid with the current SoC design methodologies.

These new types of failures are impossible to characterize using deterministic measurements so, in the near future, probabilistic metrics, such as average values and variance, will be needed to quantify the critical design objectives, such as performance and power [3]. The IPs communicates using probabilistic broadcast scheme called on-chip stochastic communication. This algorithm achieves many of the desire features of the future NoC [3] and provides:

1) Separation between computation and communication.
2) Fault- tolerance.

Despite of these features, low latency is major challenge in modern NoC. Latency in NoC can be measure by calculating the latency in switch and propagation delay in chip interconnects [4] but it depends on the type of NoC i.e. single chip NoC or multiple chip NoC (also known as Networks-in-Package). The different NoC topologies are already used in [5] and these topologies give different communication structure in NoC [6].

We proposed a method for stochastic communication, which is suitable for homogeneous as well as heterogeneous NoC. We used compartmental based stochastic communication method for Application-Specific Networks-on-Chip in, which different IPs is used. These IPs are treated as compartmental IPs moreover the flow of data from source IP to Destination IP can be represented by a compartmental network or model. From this model we can derive the compartmental matrix, which retains the properties of Metzler matrix. The derived compartmental matrix gives us the inter compartmental flow of IP cores, which help us to calculate the transition probability matrix and hence we can convert the resultant matrix into Markov Chain [7]. In IPs based compartmental models, some models are having feedback and some are not. Those models with feedback can be converted into stochastic models using Regular Markov Chains and the others using Absorbing Markov Chains. If the compartmental model is linear than we can easily generate the stochastic model, otherwise it has to be linearized using Jecobian matrix about the equilibrium points.

II. DATA FLOW NETWORK IN NOC FOR STOCHASTIC COMMUNICATION

In this section we have suggest the compartmental based probabilistic data broadcasting among the IP cores in a NoC. This process of communication is a random process. When a data in the form of packets is transmitted from source to destination IP core in the grid based square network as shown in Fig.1 then IP core communicates the data using a probabilistic broadcast scheme, similar to the randomized gossip protocols [3]. The source IP core sends the data packets to the destination IP core through its neighbors. We know that in homogeneous and heterogeneous NoC, any IP can be used as the source IP or intermediate IP or destination IP. There are many possible ways in which data can flow, depending upon the requirement.

T. Sobh et al. (eds.), Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, 11–16.

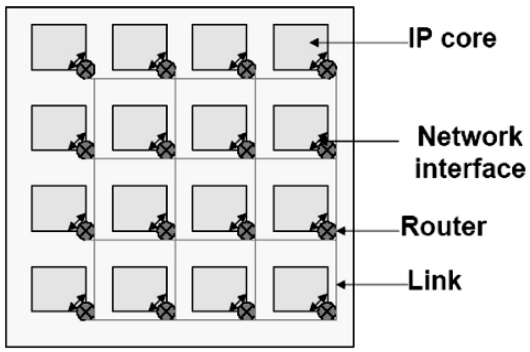

Fig. 1. Topological illustration of a 4-by-4 grid structured homogeneous NoC.

In this paper we used one of the data flow network in Application-Specific heterogeneous NoC. This NoC consist of few IPs and routers as shown in the Fig. 2.

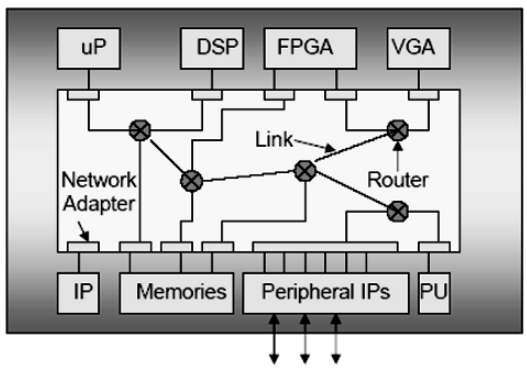

Fig. 2. Application-Specific heterogeneous NoC.

If the data has to be sent from DSP to FPGA and PU core then we can extract one of the data flow network from NoC. There are five compartments in data flow network as shown Fig. 3. These compartments are: source IP (X_1), intermediate IPs $(X_2 and\ X_3)$, and destination IPs $(X_4 and\ X_5)$.

This model of data flow network is also known as stochastic network and can be used for stochastic modeling by following certain assumptions:

1) The total number of data packets is constant.
2) The model is donor control based model.
3) The model is mass conservative.

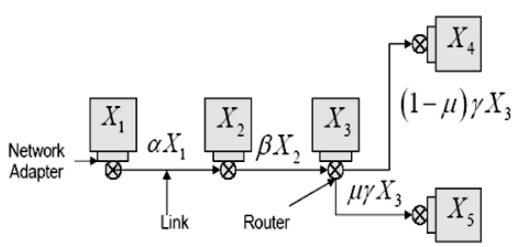

Fig. 3. Data flow network for stochastic communication.

The behavior of data flow model is shown in Fig. 3 can be described by the following set of differential equations:

$$\frac{dX_1}{dt} = -\alpha X_1 \tag{1}$$

$$\frac{dX_2}{dt} = \alpha X_1 - \beta X_2 \tag{2}$$

$$\frac{dX_3}{dt} = \beta X_2 - \gamma X_3 \tag{3}$$

$$\frac{dX_4}{dt} = (1-\mu)\gamma X_3 \tag{4}$$

$$\frac{dX_5}{dt} = \mu\gamma X_3 \tag{5}$$

$$N = X_1 + X_2 + X_3 + X_4 + X_5 \tag{6}$$

Where α, β and γ are the different data flow rates from respective compartment.

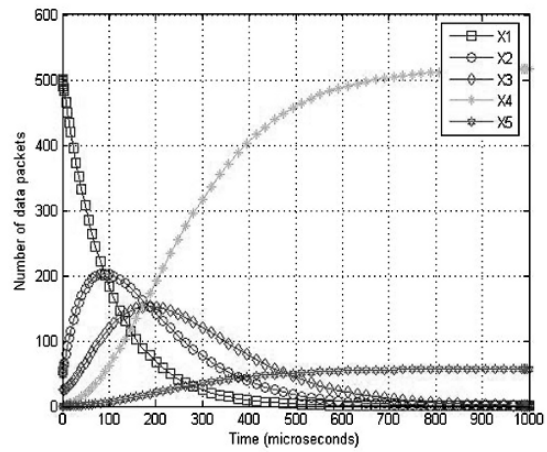

Fig. 4. Dynamic behavior of data flow network in NoC.

The dynamic behavior (number of packets transferred per unit of time) of basic data flow network in NoC is shown using Fig.4. So from here we deduce that for $N = 575$, $X_1(0) = 500, X_2(0) = 50, X_3(0) = 25$ and $X_4(0) = X_5(0) = 0$ Where N is total no. of data packets to be transmitted. For on chip synchronization all the flow rates are taken equal. $\alpha = \beta = \gamma = 0.01$. The separation constant μ is 0.1. Since the equations (1-6) describing the behavior of stochastic network and these are linear differential equations in addition to this the five compartments (X_1-X_5) can be treated as physical state space variables. Since the given set of equation is linear in nature, we can find the homogeneous solution for these equations

III. Compartmental Modeling of Data Flow Network in NoC

In this section we derived the compartmental matrix from the state space equations (1-6), defining the dynamic behavior of data flow networks (refer Fig. 4). These state space equations can be expressed in the form of matrix given below.

$$\dot{X}(t) = AX(t) \tag{7}$$

$$\begin{pmatrix} \dot{X}_1 \\ \dot{X}_2 \\ \dot{X}_3 \\ \dot{X}_4 \\ \dot{X}_5 \end{pmatrix} = \begin{pmatrix} -\alpha & 0 & 0 & 0 & 0 \\ \alpha & -\beta & 0 & 0 & 0 \\ 0 & \beta & -\gamma & 0 & 0 \\ 0 & 0 & (1-\mu)\gamma & 0 & 0 \\ 0 & 0 & \mu\gamma & 0 & 0 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \end{pmatrix} \tag{8}$$

$$A = \begin{pmatrix} -\alpha & 0 & 0 & 0 & 0 \\ \alpha & -\beta & 0 & 0 & 0 \\ 0 & \beta & -\gamma & 0 & 0 \\ 0 & 0 & (1-\mu)\gamma & 0 & 0 \\ 0 & 0 & \mu\gamma & 0 & 0 \end{pmatrix} \tag{9}$$

Where A is called compartmental matrix. The solution of this homogeneous state equation is:

$$X(t) = e^{At} X(0) \tag{10}$$

$$X(t) = \begin{pmatrix} X_1(t) \\ X_2(t) \\ X_3(t) \\ X_4(t) \\ X_5(t) \end{pmatrix} \tag{11}$$

$$e^{At} = L^{-1}\left[(sI - A)^{-1}\right] \tag{12}$$

or $$e^{At} = I + At + \frac{1}{2!}A^2t^2 + \ldots + \frac{1}{i!}A^i t^i \tag{13}$$

Where e^{At} called state transition matrix of data flow network and $X(0)$ is the column matrix which shows the initial conditions of model.

A. Properties of Compartmental Matrix

The certain important properties of compartmental matrix are retained by the matrix A, are given below:

1) The diagonal elements of compartmental matrix are zero or negative elements.
2) The non-diagonal elements of compartmental matrix are zero or positive.
3) The first eigenvalue of compartmental matrix is zero.
4) The sum of elements in each column of compartmental matrix is equal to zero.
5) Compartmental matrix is Metzler matrix.
6) It obeys the law of mass conservation

IV. Stochastic Modeling of Data Flow Network in NoC

In this section we converted the compartmental matrix A into the probability transition matrix P and obtained observing Markov Chain for stochastic modeling. Stochastic modeling is very useful to calculate the latency in NoC and also the transition probability and expected time of data flow from one IP to other IP. The transition probability matrix can be derived from compartmental matrix using following relation [8].

$$P = (I + hA)^T \tag{14}$$

The probability $p_i(n)$ that the random variable is in state i at any time n may be found from the level of numbers or quantity of random variables $x_i(n)$ in that state (now called compartment) at time n. Indeed $p_i(n) = x_i(n) \Big/ \sum_{j=1}^{k} x_j(n)$, where k is the number of states. The levels at time $n+1$ are given in terms of those at time n by the same equation,

$$X_{n+1}^T = X_n^T P, \quad n = 0,1,2,\ldots\ldots, \tag{15}$$

as the probabilities. Here, X_n is a column vector of material levels. Then, we have

$$X_{n+1}^T \begin{bmatrix} 1 \\ 1 \\ . \\ 1 \end{bmatrix} = \left[x_{n+1,1}, x_{n+1,2}, \ldots, x_{n+1,k}\right] \begin{bmatrix} 1 \\ 1 \\ . \\ 1 \end{bmatrix} = X_n^T P \begin{bmatrix} 1 \\ 1 \\ . \\ 1 \end{bmatrix} = X_n^T \begin{bmatrix} 1 \\ 1 \\ . \\ 1 \end{bmatrix} \tag{16}$$

Since $[1,1,\ldots,1]^T$ is always a right eigenvector corresponding to the steady state eigenvalue of 1 of P. If we started with a quantity $q = \sum_{j=1}^{n} x_j(0)$ of materials in the system, then the total quantity in the system remains at q for all time by (16). Thus, we have $p_i(0) = \dfrac{x_i(0)}{q.}$.

Thus, (15) is one form of equation of a compartmental system, but a more common format is as a difference equation

$$X_{n+1}^T - X_n^T = X_n^T (P - I)$$

or by taking transpose it becomes

$$\Delta X_n = \left(P^T - I\right) X_n \tag{17}$$

If the time step, i.e., the time between trials, is h rather then 1, then $X_n = X(nh)$ and the left side of (17) is replaced by the difference quotient

$$\frac{X(nh+h) - X(nh)}{h} = \frac{1}{h}\left(P^T - I\right)X(nh) = AX(nh)$$

Let $t = nh$

$$\Rightarrow \frac{X(t+h) - X(t)}{h} = AX(t)$$

This left side is approximately the derivative, so we have $X' = AX$. This is the differential equation for the

compartmental matrix and Hence $A = \frac{1}{h}\left(P^T - I\right)$, Where P the transition probability matrix and h is is the time between events or trials or more specifically $P = \left(I + hA\right)^T$.

$$P = \begin{pmatrix} 1-h\alpha & 0 & 0 & 0 & 0 \\ h\alpha & 1-h\beta & 0 & 0 & 0 \\ 0 & h\beta & 1-h\gamma & 0 & 0 \\ 0 & 0 & h(1-\mu)\gamma & 1 & 0 \\ 0 & 0 & h\mu\gamma & 0 & 1 \end{pmatrix}^T$$

$$= \begin{pmatrix} p_{x_1x_1} & p_{x_1x_2} & p_{x_1x_3} & p_{x_1x_4} & p_{x_1x_5} \\ p_{x_2x_1} & p_{x_2x_2} & p_{x_2x_3} & p_{x_2x_4} & p_{x_2x_5} \\ p_{x_3x_1} & p_{x_3x_2} & p_{x_3x_3} & p_{x_3x_4} & p_{x_3x_5} \\ p_{x_4x_1} & p_{x_4x_2} & p_{x_4x_3} & p_{x_4x_4} & p_{x_4x_5} \\ p_{x_5x_1} & p_{x_5x_2} & p_{x_5x_3} & p_{x_5x_4} & p_{x_5x_5} \end{pmatrix}$$

$$P = \begin{pmatrix} 1-h\alpha & h\alpha & 0 & 0 & 0 \\ 0 & 1-h\beta & h\beta & 0 & 0 \\ 0 & 0 & 1-h\gamma & h(1-\mu)\gamma & h\mu\gamma \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (18)$$

From (18) we can see that the sum of all elements in each row of transition probability matrix P is equal to 1. Hence

$$\sum_{j=0}^{j=4} p_{ij} = 1 \quad \text{Where i, j = 0….5} \quad (19)$$

A. Properties of Transition Probability Matrix

The certain important properties of transition probability matrix P are given below:

1) The first eigenvalue of transition probability matrix is equal to 1.
2) The sum of all elements in each row of transition probability matrix is equal to 1.
3) This matrix is also known as Markov Matrix.

B. Markov Chain from Transition Probability Matrix

The Fig. 5 shows the stochastic diagraph of transition probability matrix P.

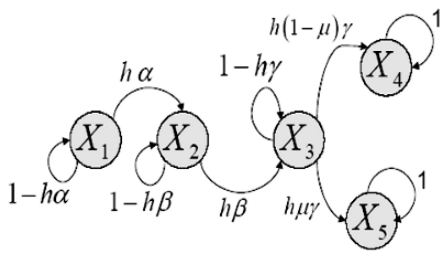

Fig. 5. Stochastic diagraph (Absorbing Markov Chain) of data flow network in NoC.

In an Absorbing Markov Chain with states ordered such that the transition probability matrix P has the form:

$$P = \begin{bmatrix} Q & R \\ 0 & I \end{bmatrix} \quad (20)$$

And the following hold:

1) $Q^t \to 0$ as $t \to \infty$.
2) $R_\infty = \left(I - Q\right)^{-1} R$.
3) The expected number of times a chain is in the non absorbing state k_j given that it started in k_i is given by the corresponding element of $\left(I - Q\right)^{-1}$.

The matrix $\left(I - Q\right)^{-1}$ is often referred to as *Markov chain's fundamental matrix* for each non absorbing state, there is an absorbing state with a path of minimum length. Let r be the maximum length of all such paths. Therefore, in r steps, there is a positive probability p of entering one of the absorbing states regardless of where you started. The probability of not reaching an absorbing state in r *steps* is $\left(I - p\right)$. After the next r steps, it is $\left(I - p\right)^2$ and after kr steps, $\left(I - p\right)^k$. Since this approaches 0 as $k \to \infty$, the probability of being in any non absorbing state approaches 0 as $t \to \infty$. But the elements of Q^t are just these probabilities. In this paper $\left(I - Q\right)^{-1}$ will give us the expected time of data flow from one IP core to other IP core. And $R_\infty = \left(I - Q\right)^{-1} R$ will give us the probability of data transmission to the destination IP core.

V. Stochastic Analysis of on Chip Communication

In this section we verified the compartmental based stochastic communication scheme. From (18) and (20), we get

$$P = \begin{bmatrix} Q & R \\ 0 & I \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} 1-h\alpha & h\alpha & 0 \\ 0 & 1-h\beta & h\beta \\ 0 & 0 & 1-h\gamma \end{bmatrix} & \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ h(1-\mu)\gamma & h\mu\gamma \end{bmatrix} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix}$$

The last state of this Markov Chain I is the absorbing state which consists of destination IPs in NoC. For $\alpha = \beta = \gamma = 0.01$ and μ is 0.1.The time for each event or transition h is 0.1. This implies

$$P = \begin{bmatrix} 0.999 & 0.001 & 0 & 0 & 0 \\ 0 & 0.999 & 0.001 & 0 & 0 \\ 0 & 0 & 0.999 & 0.0009 & 0.0001 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$Q=\begin{bmatrix} 0.999 & 0.001 & 0 \\ 0 & 0.999 & 0.001 \\ 0 & 0 & 0.999 \end{bmatrix},\ R=\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0.0009 & 0.0001 \end{bmatrix},$$

$$I=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

For transient response

$$\left(I-Q\right)^{-1}=\begin{bmatrix} 1000 & 1000 & 1000 \\ 0 & 1000 & 1000 \\ 0 & 0 & 1000 \end{bmatrix}$$

From $\left(I-Q\right)^{-1}$ matrix we can calculate:

1) Expected time during which the data available with source IP core $\left(X_1\right)$ = 1000 microseconds.
2) Expected delay to reach the intermediate IP $\left(X_3\right)$ = 1000 + 1000 = 2000 microseconds.
3) Expected time during which the data live on intermediate IP core $\left(X_3\right)$ = 1000 microseconds.
4) Expected delay to reach from intermediate IP $\left(X_2\right)$ to the destination IP $\left(X_4\right)$ = 1000 + 1000 = 2000 microseconds.
5) Expected delay to reach from source IP $\left(X_1\right)$ to the destination IP $\left(X_4\right)$ = 1000 + 1000 + 1000 = 3000 microsecond.

For steady state response

$$R_\infty=\left(1-Q\right)^{-1}R=\begin{bmatrix} 0.9 & 0.1 \\ 0.9 & 0.1 \\ 0.9 & 0.1 \end{bmatrix}$$

From $R_\infty=\left(1-Q\right)^{-1}R$ matrix we can calculate:

1) Probability of data reception by IP X_4 = 0.9.
2) Probability of data reception by IP X_5 = 0.1.

For the steady state, complete transition probability matrix is

$$P_\infty=\begin{bmatrix} Q_\infty & R_\infty \\ 0 & I \end{bmatrix}$$

$$P_\infty=\begin{bmatrix} 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

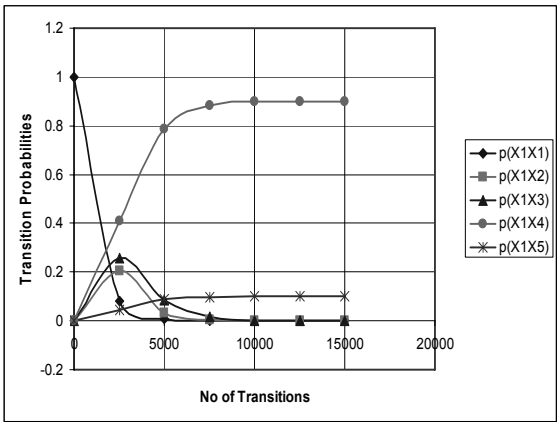

Fig. 6. Transition probabilities of data flow for IP $\left(X_1\right)$

TABLE I

TRANSITION PROBABILITIES OF DATA FLOW FOR IP $\left(X_1\right)$

No. of Transitions	Transition probabilities				
	p(X1X1)	p(X1X2)	p(X1X3)	p(X1X4)	p(X1X5)
1	0.999	0.001	0	0	0
2500	0.082	0.2052	0.2566	0.4106	0.0456
5000	0.0067	0.0336	0.0842	0.7879	0.0875
7500	0.0006	0.0041	0.0155	0.8818	0.098
10000	0	0.0005	0.0023	0.8975	0.0997
12500	0	0	0.0003	0.8997	0.1
15000	0	0	0	0.9	0.1

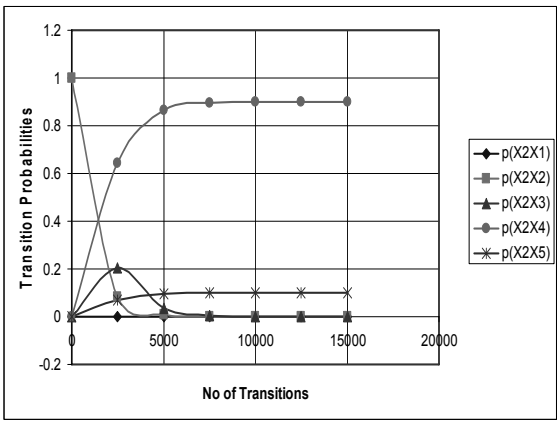

Fig. 7. Transition probabilities of data flow for IP $\left(X_2\right)$

TABLE II

TRANSITION PROBABILITIES OF DATA FLOW FOR IP $\left(X_2\right)$

No. of Transitions	Transition probabilities				
	p(X2X1)	p(X2X2)	p(X2X3)	p(X2X4)	p(X2X5)
1	0	0.999	0.001	0	0
2500	0	0.082	0.2052	0.6416	0.0713
5000	0	0.0067	0.0336	0.8637	0.096
7500	0	0.0006	0.0041	0.8958	0.0995
10000	0	0	0.0005	0.8996	0.1
12500	0	0	0	0.9	0.1
15000	0	0	0	0.9	0.1

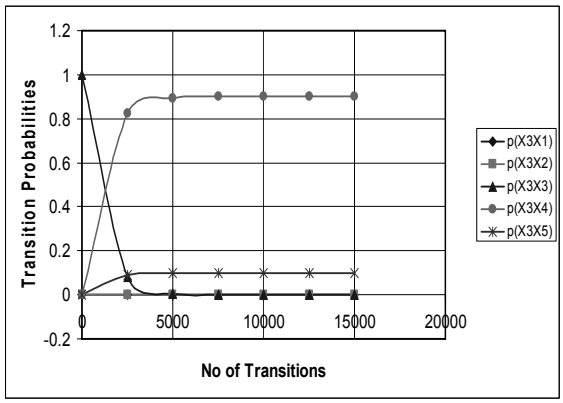

Fig. 8. Transition probabilities of data flow for IP (X_3)

TABLE III

TRANSITION PROBABILITIES OF DATA FLOW FOR IP (X_3)

No. of Transitions	Transition probabilities				
	p(X3X1)	p(X3X2)	p(X3X3)	p(X3X4)	p(X3X5)
1	0	0	0.999	0.0009	0.0001
2500	0	0	0.082	0.8262	0.0918
5000	0	0	0.0067	0.894	0.0993
7500	0	0	0.0006	0.8995	0.0999
10000	0	0	0	0.9	0.1
12500	0	0	0	0.9	0.1
15000	0	0	0	0.9	0.1

In Fig. (6-8) and Table (I-III), P (XiXj) shows the transition probabilities of data flow from one Xi IP core to Xj IP core where i = 1..3 and j=1..5. From this stochastic model we can calculate the total transition probabilities between any two IP cores, which is very useful to calculate the latency. In addition to this the proposed method makes separation between communication and computation.

VI. CONCLUSION AND FUTURE WORK

In this paper we have proposed a new method for stochastic communication between the different IP (Intellectual Property) cores. In addition to this our method helps in building the compartmental model of IPs on the NoC and moreover calculating the latency as well as the transition probabilities of data flow between any two IPs. From the Fig. 6-8 and Tables (I-III) it is depicted that the transient and steady state response of transition probabilities gives us the state of data flow latencies among the different IPs in NoC.

In future the work presented here can be applied on any kind of on-chip interconnects topology. In addition to this we can find out the controllability and absorbability for each NoC and can design a condensed compartmental network for stochastic communication in NiP. The method for stochastic modeling is very useful to calculate the latency only if; we use the inflow and outflow in a NoC in NiP architecture. We can use this work to merge the two kind of communications one is inter NoC and another is inter NiP.

ACKNOWLEDGEMENT

The authors would like to thank the editor and the anonymous reviewers for their constructive comments and suggestions that significantly improved the quality of the paper. Finally we would like to thank Professor Ashok Subramanian PhD (CS – Stanford University USA) for his moral support and technical inputs.

REFERENCES

[1] L. Kangmin, L. Se-Joong, K. Donghyun, K. Kwanho, K. Gawon, K. Joungho, and Y. Hoi-Jun, "Networks-on-chip and Networks-in-Package for High-Performance SoC Platforms," *IEEE* pp. 485-488, 2005.

[2] L. Kangmin, L. Se-Joong and Y. Hoi-Jun, "Low-Power Network-on-Chip for High-Performance SoC Design," *IEEE Transactions On Very Large Scale Integration (VLSI) Systems, Vol. 14, No. 2*, pp. 148-160, February 2006.

[3] D. Tudor and M. Radu, "On-Chip Stochastic Communication," *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition,* 2006.

[4] K. Kwanho, L. Se-Joong, L. Kangmin and Y. Hoi-Jun, "An Arbitration Look-Ahead Scheme for Reducing End-to-End Latency in Networks on chip," *IEEE*, pp. 2357-2360, 2005.

[5] S. Murali, and G. Micheli, "SUNMAP: A Tool for Automatic Topology Selection and Generation for NoCs," *IEEE DAC*, San Diego, California, USA, pp. 914-919, June 7–11, 2004.

[6] T. Bjerregaard and S. Mahadevan, "A Survey of Research and Practices of Network-on-Chip, "*ACM Computing Surveys, Vol. 38, Article 1*, pp. 1-51, March 2006.

[7] V. K. Sehgal, "Stochastic Modeling of Worm Propagation in Trusted Networks," *SAM,* Las Vegas, USA, pp. 482-488, June 26-29, 2006.

[8] G. Gilbert, Walter and Martha Contreras, "Compartmental Modeling with Networks". *Morgan-Kauffman,* 2000.

A Random Approach to Study the Stability of Fuzzy Logic Networks

Yingjun Cao, Lingchu Yu, Alade Tokuta
Department of Mathematics & Computer Science
North Carolina Central University
Durham, NC 27707
ycao@nccu.edu, lyu@mail.nccu.edu, atokuta@nccu.edu

Paul P. Wang
Department of Electrical & Computer Engineering
Duke University
Durham, NC 27708
ppw@ee.duke.edu

***Abstract*-In this paper, we propose a general network model, fuzzy logic network (FLN), and study its stability and convergence properties. The convergence property was first deduced theoretically. Then a random approach was adopted to simulate the convergence speed and steady-state properties for a variety of fuzzy logical functions. The simulation results show that MV logical function causes the system to be on the edge of chaos when the number of nodes increases. Thus this logical function is more useful to infer real complex networks, such as gene regulatory networks.**

I. INTRODUCTION

One of the most challenging problems in bioinformatics is to determine how genes inter-regulate in a systematic manner which results in various translated protein products and phenotypes. To find the causal pathways that control the complex biological functions, researchers have been modeling gene regulatory mechanisms as a network topologically in order to gain more detailed insight [1]. It, in return, arouses the need of novel network models. The importance of the networking model is that normal regulatory pathways are composed of regulations resulting from many genes, RNAs, and transcription factors (TFs). The complicated inter-connections among these controlling chemical complexes are the driving force in maintaining normal organism functions. The simplest yet commonly used model for gene regulatory networks is the so called *NK* Boolean network [2]. It is a directed graph to model the situation where gene *A* and gene *B* interact during some time intervals and their interactions will determine or regulate the status of another gene *C* through a Boolean logical function at the next step. If numerous genetic regulations occur simultaneously, the participating genes with their unique logical functions form the components of a gene regulatory network. This network will be self-evolutionary and eventually reach certain final states. In the *NK* network nomenclature, *N* is the total number of genes in the network, and *K* denotes the maximum number or the average number of regulating genes. The *NK* Boolean network theory has been carried out in a variety of ways both in deduced mathematical approximation and computer simulations [2-4]. Due to the binary limitation inherent in Boolean values, however, the exact properties of gene regulation cannot be expressed in detail based on this model. Thus other approaches were adapted to model the gene regulation mechanism, such as differential equations [5], Bayesian networks [6], and genetic circuits [7]. These models, however, have stressed different aspects of the regulatory behavior, and each model has contributed good inference results in certain aspect of the issue. The ongoing research on those models has focused on non-linear data processing, noise tolerance, and model over fitting [8].

In this paper, we propose and study a general network model, the fuzzy logic network (FLN) which is believed to possess the capacity of modeling complex networks and self-organizable systems, such as biological or economical systems. In a sense, the FLN is the generalization of Boolean network, but is capable of overcoming the unrealistic constraint of Boolean value (ON/OFF symbolically). Fuzzy logic has evolved as a powerful tool over 40 years, and its applications are widely available in scientific research and engineering literature. The proposed FLN is able to inherit all the good properties of Boolean networks, especially the causal property in the dynamic network behavior. Additionally, it is also expected to be a more effective model with the nuance of membership function adjustment and inference rules. The FLN also has numerous known advantages such as modeling the highly non-linear relationships and periodicity. With distinctive properties in processing real-life incomplete data and uncertainties, the gene regulation analysis based on fuzzy logic theory did emerge after 2000 [9] and some good developments have been documented since then [10-16].

The general study of FLN's convergence and stability presented in this paper is organized as follows. In section II, the FLN's definitions and their appropriate meanings are given. Two important theorems concerning the evolutionary property of the FLN are proved. In section III, the simulation algorithm is illustrated. In the following section, the simulation results are presented and discussed in detail. Conclusions and future research are discussed in section V.

II. FUZZY LOGIC NETWORK

A. Definitions

1) Fuzzy logic network

Given a set of N fuzzy variables (genes), $\vec{X}_t = [x_t^1, x_t^2, \cdots, x_t^N], x_t^i \in [0,1], i \in \underline{N}$, index t represents time; the variables are updated by means of dynamic equa-

T. Sobh et al. (eds.), Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, 17–21.

tions, $x_{t+1}^{i} = f_i(x_t^{i_1}, x_t^{i_2}, \cdots, x_t^{i_K})$ where f_i is a randomly chosen fuzzy logical function.

In the FLN, the fuzzy logical functions can be constructed using the combination of AND, OR,←and COMPLEMENT. The total number of choices for fuzzy logical functions is decided only by the number of inputs. If a node has $K(1 \le K \le N)$ inputs, then there are 2^{2^K} different fuzzy logical functions. In the definition of FLN, each node x_t^i has K inputs on average.

2) Fuzzy logical functions

Fuzzy logical function is a binary operation that satisfies the identity, commutative, associative and increasing properties. A fuzzy logical function usually has to satisfy the so called **t-norm/t-co-norm**. Table I is a list of commonly used fuzzy logical functions with the AND, OR and COMPLEMENT [17].

TABLE I
COMMONLY USED FUZZY LOGICAL FUNCTIONS

Fuzzy Logical Function	$a \wedge b$	$a \vee b$	$\bar{a}$
Max-Min	$\min(a,b)$	$\max(a,b)$	$1-a$
GC	$a \times b$	$\min(1, a+b)$	$1-a$
MV	$\max(0, a+b-1)$	$\min(1, a+b)$	$1-a$
Probabilistic	$a \times b$	$a+b-a \times b$	$1-a$

3) Quenched update

If all the fuzzy logical functions, $f_i (i \in \underline{N})$, and their related variable set, $\{x_t^{i_1}, x_t^{i_2}, \cdots, x_t^{i_K}\}$, chosen at the initial state of the system remain the same throughout the whole dynamic process, then the system is termed as quenched updated.

4) Synchronous update

If all the fuzzy variables, x_t^i, are updated at the same time, then the system is called synchronously updated; otherwise, it is asynchronously updated. In this paper, the FLN is assumed to be synchronously updated.

5) Basin of attraction

It is the set of points in the system state space, such that initial conditions chosen in this set dynamically evolve toward a particular steady state.

6) Attractor

It is a set of states invariant under the dynamic progress, toward which the neighboring states in a given basin of attraction asymptotically approach in the course of dynamic evolutions. It can also be defined as the smallest unit which cannot be decomposed into two or more attractors with distinct basins of attraction.

7) Limit cycle

It is an attracting set of state vectors to which orbits or trajectories converge, and upon which their trajectories are periodic.

B. Theorems

Theorems in this section have focused on the dynamical convergence process of the FLN. The reason is not all FLNs have limit cycles or attractors as strictly as in the case of Boolean. Excellent work has been done in Boolean Network on the characteristics of the cycles [18-19], but it has been shown that power law appears when the system has exponentially short cycles locally. The length of cycles and the number of cycles are heavily affected by the chaotic property. This property arouses the motivation to simulate the convergence of randomly FLNs.

Theorem 1: Quenched FLN using the Max-Min logical function must reach limit cycles or attractors

Proof:

If the initial conditions of the network are $\vec{X}_1 = [x_1^1, x_1^2, \cdots, x_1^N]$, and the Max-Min logical function is used, it is obvious that the possible values of any variable, x_t^i, at any time t can be only selected from

$$\{x_1^1, 1-x_1^1, x_1^2, 1-x_1^2 \cdots, x_1^N, 1-x_1^N\}$$

So the state space initially includes maximally $2N$ possible values (some values out of $2N$ may be the same so $2N$ is the upper limit). Since the FLN is quenched, the initial configurations will remain the same throughout the whole dynamic process. So the state space remains the same, which are all the possible iterations of $2N$ values on a $N \times 1$ vector space. Thus the state space includes maximally $(2N)^N$ different vectors.

After $(2N)^N$ updates at most, the network must have reached a state where it has already visited. So the network must have limit cycles or attractors.

This property is only valid for the quenched network using the Max-Min logical function. If other types of logical functions (GC, MV or Probabilistic shown in Table I) are used, then the network cannot be guaranteed to reach exact limit cycles or attractors. Take GC logical function as an example. A simple two variable network, $\{x_t^1, x_t^2\}$, has the following update rules.

$$x_{t+1}^1 = x_t^1 \wedge x_t^2$$
$$x_{t+1}^2 = x_t^2$$

Suppose the initial value is $\{x_1^1 = 0.2, x_1^2 = 0.5\}$, then the network will evolve through the following states:

$$(0.2, 0.5) \to (0.2 \times 0.5, 0.5) \to \cdots (0.2 \times 0.5^i, 0.5) \cdots .$$

As can be seen, it will never reach a previously visited state because the value of the first variable at the current time is always different from any of its ancestors. However, one trend can be seen is that although some FLNs will not reach the exact steady state, the network can be thought as reaching a pseudo-steady state asymptotically. In this example, the pseudo steady state is $(0, 0.5)$. However, the convergence properties of FLNs based on different logical functions are unknown. We have found that given a precision, all FLNs we simulated converged. Fig.1 shows examples of convergence based on the four logical functions shown in Table I.