Journal of Advances in Computer Research
Quarterly pISSN: 2345-606x eISSN: 2345-6078
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 5, No. 2, May 2014), Pages: 71-80
www.jacr.iausari.ac.ir

Presenting a Fault Tolerant Mechanism for Buffering Fault in Network on Chips

Sadeq Lotfi[1] *, Ali Afzali-kusha[2], Marzie Saffari[3]

(1), (3)Department of Computer Engineering Arak Branch, Islamic Azad University, Arak, Iran
(2)Professor, Department of Electronic Engineering, Tehran University, Tehran, Iran
sadeqLotfi@gmail.com, aafzali05@gmail.com, marziesaffari@gmail.com

Received: 2013/12/07; Accepted: 2014/01/19

Abstract

As technology scales deep into the nanometer regime, on-chip communication becomes more susceptible to transient noise sources, such as crosstalk, external radiation, and spurious voltage spikes. The Network on chip s modularity and reusability has brought about the use of error control methods to address transient errors in Network on chip links.In this work, we design a fault tolerance router with efficient area and power dissipated. Actually, we exploit the free virtual channel to store the redundant data. Virtual channel is used for deadlock avoidance it can be implement as 2, 4 or 8 channel. The almost time we can find a free channel that we can use in fault tolerance mechanism. We describe the proposed architecture with VHDL and implemented with synopsis compiler design. We use analytical model to evaluate the fault tolerance. The result shows that we improve the dynamic power dissipation, area, and reliability.

Keywords: *Network on chip, Buffering, Virtual channel, Fault tolerance router*

1. Introduction

Shrinking of circuit capacitors capacity and decreasing of voltage levels, Power supply, Logic, Gate sensitivity, Flip-Flops and memory unit systems become vulnerable against various environment noises, charged particles and cross talk noises. These factors leading to cause transient or permanent faults in the system. For this reason, designing the fault tolerance system that can prevent fault results or destructive effects or using strategies can retrieve themselves from caused fault in system is very important. The use of transistors on a chip is important from two aspects. First, costs design, structure, verification, and test of chips will increase according to inefficient components and communication structures fault tolerance factor that complemented on chips is very important. The other aspect is that more complicated design, increase the probability of occurring human fault in time of designing and implementation so elimination and examination them in verification method require more costs.

According to the expressed issues, the designing of network on chip that use not only better method to increase reliability, and the probability of retraining and fault tolerance. So recognizing human fault and solving them, is very important.

2. Related Work

To resist network on chip against the transient faults, detection method or fault correction is used. Because usual methods that use hardware or time redundancy are not affordable. In [1], [2] Frantz invented methods to tolerant two simultaneously faults according to required overload and interaction. These methods by fault correction codes and hardware and time redundancy prevent faults in output that cause because of occurring of SEU1 and interaction. In [3] by using triple repetition of fault correction codes and a special coding to prevent interaction fault, has achieved to reliability with reducing of power consumption. The examples of related researches with architectures designing of fault tolerance for routers, has been implemented by Kim [4], [6-7]. In [۷] a set of many methods presented to preserve fault source in network on chip such as transient fault in links and SEU fault in router. In this method some strategies have been used such as resource sharing to reduce overload. In [8] by using backup routing, path has prevented faulty nodes and has preserved communications and connections. In [10] a method presented, that used a mechanism of virtual channel in router structure to solve blocking problem in buffer. Using this channels increase complication of designing and buffers controlling. Virtual channel by multiplexing many logical channels on a physical channel solve blocking problem and increase links efficiency.

3. The method of buffering fault tolerance in network on chip

3.1 Triple redundancy method

In this method to detect fault of each data, we can save input in three corresponding cells of parallel buffer and compare them when data exited. While data are different, we can recognize fault in one of the data. To correct the fault, we can compare data when they are from buffers and if there is a difference, select a data that the majoring voted to it.

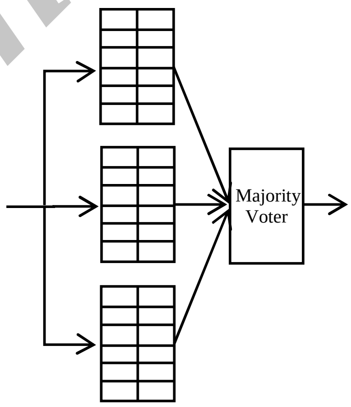

Figure1. Input buffering with Triple redundancy method

3.2SECDED[2] data redundancy method

[1] Single Event Upset

[2] Single Error Correction Double Error Detection

In this method, the purpose is adding a code to original data. By adding code, we can recognize the fault of data and correct them in destination.

As seen in the Figure2, the bit of original data with the controlling bit flow in circuit. To increase fault tolerance in network on chip router, encoder and decoder modules have been used. The encoder and decoder modules location in this design is such that we are able to correct and recognize occurred faults on communication links. In this method, data with syndrome bits saved temporary in input buffer and controlling done, while the data exited from buffering. By this method, we can recognize two faults and modify one fault [5].

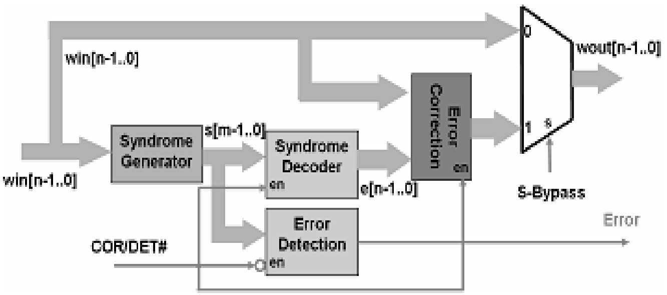

Figure2. Input buffering with SECDED method[5]

3.3FTSECDED[1]proposed method

In this method we used available and useless hardware instead of adding additional hardware. In designing of network on chip router, input buffer implemented as virtual channel. Virtual channels are used to avoid deadlock and to eliminate blocking problem. In routers working by XY routing algorithm and having 5ports,the using of virtual channel is not the same, and in most of the time is empty and useless [10]. The data in propose method, is separated in two data and data check. Data and data check enter by previous router or VC0, VC1virtual channels. This method is able to correct a fault and detect two data faults. Correction and detection of fault implemented in decoder and encoder. As one fault detected, the data is corrected.As two faults recognized in data, error resist pin can be active and the requesting of sending data back is sent to previous router.

[1] Fault Tolerant Single Error Correction Double Error Detection

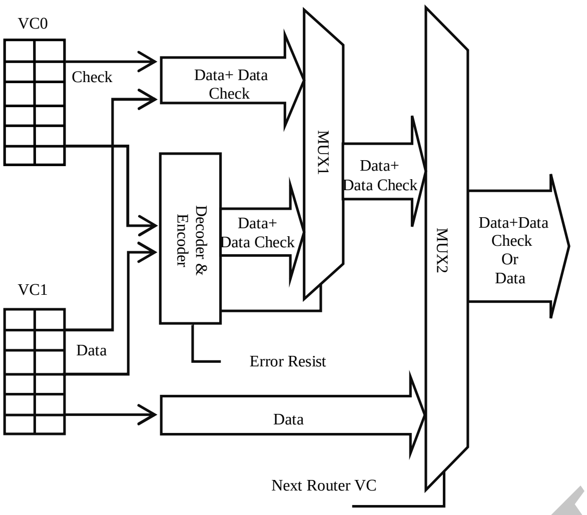

Figure3. Input buffering with FTSECDED method

Used algorithm is as follow:

```
If Error Resist
  Assert “Error-Retransmission Request”
ElseIfnext_router_vcIs free
      If Data+DataCheckIs ready
Send(Data+DataCheck)
      Else
         Compute DataCheck
Send(DataCheck)
  Else
Send (Data)
```

In current router we control that arrived data is normal or not. If arrived data is not normal, requesting of sending data will be sent back sent to previous router. As a normal data arrived to router and no error or faults delivered in arrived data. Then the availability of free virtual channel for data check in next router is controlled. If virtual channel is not tree, the original data will only send. The controlling data is not transferred with original data to next router.

On the other hand, if free virtual channel is available in current router, arriving of data check is checked. If the data check is not arrived from previous router, data check will computed by original data and will sent with data to next router. If the data check is arrived from previous router is would, not computed again and will sent with original data to next router.

If virtual channel be free or *next_router_vc* be active, this part should examine that data check as well as original data has arrived from previous router or not. If data check is not arrived, that data check as well as original data has arrived from previous router or not. If data check is not arrived, data check is computed by original data and guided to MUX2 for sending to next router by controlling of activation pin in MUX1.

4. Testing and Evaluation

Above methods are implemented by CAD Tools and their reliability are examined.

4.1 synthesis by CAD Tools

In this section, TMR, SECDED, FTSECDED methods are compared from points of occupancy level by compositional and non-compositional elements, critical path and power consumption. The compositional elements such as AND, OR, Gates and non-compositional elements such as Flip-Flops. The critical path is the path with maximum delay in circuit. Power consumption of circuits is divided to static and dynamic. The dynamic power consumption is the power consumption in active circuit and is divided to switching and external.

According to Table1, in occupancy level of compositional circuits, the proposed method is located after SECDED method and the lowest space is for the non-compositional circuit. FTSECDED have the shorter path in critical path. In total, it is better as total power consumption and dynamic power consumption than the other method. It has only more leakage power there is SECDED method.

Table1. CAD Tools Result

	Com Area	NonCom Area	Critical Path	Dynamic Power	Leakage Power	Total Power
FTSECDED	4.61um^2	7.83um^2	0.25 ns	6.41mw	213uw	6.62mw
SECDED	3.22um^2	8.68um^2	0.28 ns	7.81mw	190uw	8.00mw
TMR	5.08um^2	14.5um^2	0.28 ns	14.0mw	320uw	14.4mw

4.2 Reliability

The reliability computed by evaluating burst and random error.P(n) in formula 1, is the probability of occurring random error.

$$P(n)=(1\text{-}p_n)^2*\varepsilon*P_{(\text{Channel Width*Packet Size}),\text{Number of Error}} \qquad (1)$$

εis the probability of occurring random error in one link, assumed 0.01 in evaluations.$p_n$is the probability effect of one defected link on neighbor links.$P_{(\text{Channel Width}*\text{Packet Size}),\text{Number of Error}}$is the permutation or the number of occurring mode of one random occurring that is the channel witch and it is assumed 8 in computations. The maximum number of error is equal to channel width. Packet size is the number of flit that a packet is divided to these numbers.

The introducing of P (N,B,R) is necessary, Because it shows the possibility of occurring N errors that B errors are burst error and R errors are random errors. Also P(N,B1#B2,R), that B1,B2 are the number of burst errors, and occur in two points. For example, evaluate (2,2,0) mode that two errorsoccurin system. That both of there are burst errors. To be more precise, are burst errors. To be more precise, a random error occurred in system and be case to occur a burst error in one of the neighbor system. The possibility of error computed by formula2:

$$P(2,2,0)=\binom{2}{1}*p_n(1\text{-}p_n)*\frac{P(1)}{(1\text{-}p_n)^2} \qquad (2)$$

P(1) is the possibility of occurring of random error and when it is divided on (1-p_n)2, the possibility of being non burst is omitted. p_n(1-p_n) is only for that occurred error can be cause one burst error in one of the two neighbor systems. The $\binom{2}{1}$ means that occurring of burst error occur by selecting one of the modes.

$$\mathrm{P}(3,3,0)=\mathrm{p_n}^{2}*\frac{\mathrm{P}(1)}{(1\text{-}\mathrm{p_n})^2} \quad (3)$$

$$\mathrm{P}(3,2,1)=\binom{2}{1}*\mathrm{P}(2,2,0)*\frac{\mathrm{P}(1)}{(1\text{-}\mathrm{p_n})^2} \quad (4)$$

$$\mathrm{P}(4,3,1)=\binom{2}{1}*\mathrm{P}(3,3,0)*\frac{\mathrm{P}(1)}{(1\text{-}\mathrm{p_n})^2} \quad (5)$$

$$\mathrm{P}(4,2,2)=\mathrm{P}(2,2,0)*\binom{3}{1}*\frac{\mathrm{P}(2)}{(1\text{-}\mathrm{p_n})^4} \quad (6)$$

$$\mathrm{P}(4,2\#2,0)=\mathrm{P}(2,2,0)^2 \quad (7)$$

$$\mathrm{P}(5,3\#2,0)=\binom{2}{1}*\mathrm{P}(2,2,0)*\mathrm{P}(3,3,0) \quad (8)$$

$$\mathrm{P}(5,2\#2,1)=\binom{3}{2}*\mathrm{P}(2,2,0)^{2}*\frac{\mathrm{P}(1)}{(1\text{-}\mathrm{p_n})^2} \quad (9)$$

$$\mathrm{P}(5,2,3)=\binom{4}{1}*\mathrm{P}(2,2,0)*\frac{\mathrm{P}(3)}{(1\text{-}\mathrm{p_n})^6} \quad (10)$$

$$\mathrm{P}(5,3,2)=\binom{2}{1}*\mathrm{P}(2,2,0)*\frac{\mathrm{P}(2)}{(1\text{-}\mathrm{p_n})^4} \quad (11)$$

The computing of probability of error in SECDED, FTSECDED, TMR, and No Coding done as follow:

- ***No Coding***

In this method, arrived flit to router, sent to next router without a mechanism for fault tolerance. So the possibility of total error modes added and the result will be formula12.

$$\mathrm{P(NoCoding)}=\sum_{i=1}^{5}\mathrm{P(i)}+\text{All Burst Error Probability} \quad (12)$$

- ***TMR***

In this method, all one-bit errors are detectable and correctable.The possibility of one third can recognize more than one-bit errors. One third is due to that by this possibility error may occur more than one number in that destroyed Flit. So, by the formula 13, error is computed the possibility of this mode:

$$\mathrm{P(TMR)}=\left(1\text{-}\frac{1}{3}\right)*\sum_{i=2}^{5}\mathrm{P(i)}+\text{AllBurstErrorProbability} \quad (13)$$

- ***SECDED***

In this method, the ability of detection of more than two errors is not possible. So, formula 14 that is total random errors possibility and all modes of burst errors except (2,2,0), will be error occurring possibility in this mode.

$$\mathrm{P(SECDED)}=\sum_{i=3}^{5}\mathrm{P(i)}\ +\text{All Burst Error Probabilities Except }\mathrm{P}(2,2,0) \quad (14)$$

- ***FTSECDED***

In this method, recognize triple random errors are seven of eight. If three errors were in the same section, this method could not recognize three errors. Also, the below modes are recognizable in burst errors. We can say, the possibility of occurring 3errors in one second from two sections, is equal one second triple or one eighth. Also the following modes are recognizable in quiver error. Total errors of (2.2.0) mode, third-quarters errors of (3.2.1) mode and third-quarters errors of (4.2.2) mode, because the one-second possibility, May occur two random errors and one of them may be changed to two quiver errors. One second errors of (3.3.0) mode, because the one second possibility, the random error occur in wire which cause the possibility of occurring this error mode in one section. The possibility of FTSECDED,SECDED,TMR,NoCoding errors by changing packet size.

$$\mathrm{P(FTSECDED)} = \left(\frac{1}{2}\right)^3 * \mathrm{P}(3) + \sum_{\mathrm{i}=4}^{5} \mathrm{P(i)} + \text{All Burst Error Probabilities Except} \mathrm{P}(2,2,0) + \frac{3}{4}\mathrm{P}(3,2,1) + \frac{1}{2}\mathrm{P}(3,3,0) + \frac{3}{4}\mathrm{P}(4,2,2) \quad (15)$$

4.3 Reliability evaluation

First, the effect of this factor on error possibility is evaluated in four methods, by changing the value of εfrom 1.00E-6+1.00E-14. Table2 and figure 4 show the result of this evaluation, NoCoding is inefficient method. TMR is better than NoCoding method but it is not better than FTSECDED, SECDED with changing the packet size from 4 to 20 and computing the error possibility, the evaluation is continued.Table3 and figure 5show the evaluation. The results show that NoCoding and TMR methods are poor efficient than SECDED and FTSECDED, also FTSEDED is better than SECDED.

Table 2. Fault probability of NoCoding, TMR, SECDED and FTSECDED with ε change

ε	NoCoding	TMR	SECDED	FTSECDED
1.00E-06	3.20E-05	4.25E-07	3.24E-09	2.14E-09
1.00E-07	3.20E-06	4.25E-08	3.20E-10	2.13E-10
1.00E-08	3.20E-07	4.25E-09	3.20E-11	2.13E-11
1.00E-09	3.20E-08	4.25E-10	3.20E-12	2.13E-12
1.00E-10	3.20E-09	4.25E-11	3.20E-13	2.13E-13
1.00E-11	3.20E-10	4.25E-12	3.20E-14	2.13E-14
1.00E-12	3.20E-11	4.25E-13	3.20E-15	2.13E-15
1.00E-13	3.20E-12	4.25E-14	3.20E-16	2.13E-16
1.00E-14	3.20E-13	4.25E-15	3.20E-17	2.13E-17

In fact by increasing the packet size, the error possibility will increase and is proved by formula1.If p_n is assumed zero, the possibility of burst error occurring is eliminated. Therefore, the possibility of random errors occurring is evaluated. Table 4 and figure 6 show the related data.

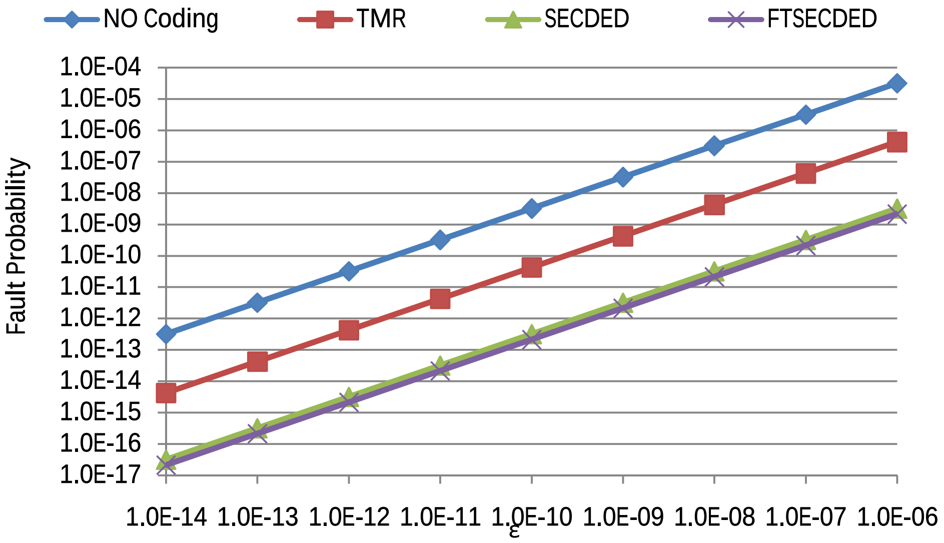

Figure 4. Fault probability of NoCoding, TMR, SECDED and FTSECDED with ε change

Table 3. Fault probability of NoCoding, TMR, SECDED and FTSECDED with packet size change

PacketSize	NoCoding	TMR	SECDED	FTSECDED
4	3.20E-11	4.25E-13	3.20E-15	2.13E-15
6	4.80E-11	6.37E-13	4.80E-15	3.20E-15
8	6.40E-11	8.49E-13	6.40E-15	4.26E-15
10	8.00E-11	1.06E-12	8.00E-15	5.33E-15
12	9.60E-11	1.27E-12	9.60E-15	6.39E-15
14	1.12E-10	1.49E-12	1.12E-14	7.46E-15
16	1.28E-10	1.70E-12	1.28E-14	8.52E-15
18	1.44E-10	1.91E-12	1.44E-14	9.59E-15
20	1.60E-10	2.12E-12	1.60E-14	1.07E-14

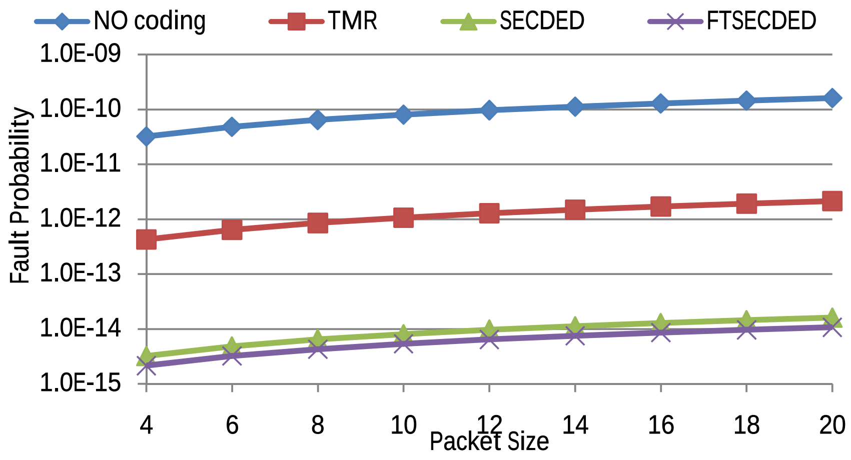

Figure 5. Fault probability of NoCoding, TMR, SECDED and FTSECDED with packet size change

Table 4. Fault probability of NoCoding, TMR, SECDED and FTSECDED with p_n=0

ε	NoCoding	TMR	SECDED	FTSECDED
1.00E-06	3.20E-05	3.31E-10	4.96E-15	6.20E-16
1.00E-07	3.20E-06	3.31E-12	4.96E-18	6.20E-19
1.00E-08	3.20E-07	3.31E-14	4.96E-21	6.20E-22
1.00E-09	3.20E-08	3.31E-16	4.96E-24	6.20E-25
1.00E-10	3.20E-09	3.31E-18	4.96E-27	6.20E-28
1.00E-11	3.20E-10	3.31E-20	4.96E-30	6.20E-31
1.00E-12	3.20E-11	3.31E-22	4.96E-33	6.20E-34
1.00E-13	3.20E-12	3.31E-24	4.96E-36	6.20E-37
1.00E-14	3.20E-13	3.31E-26	4.96E-39	6.20E-40

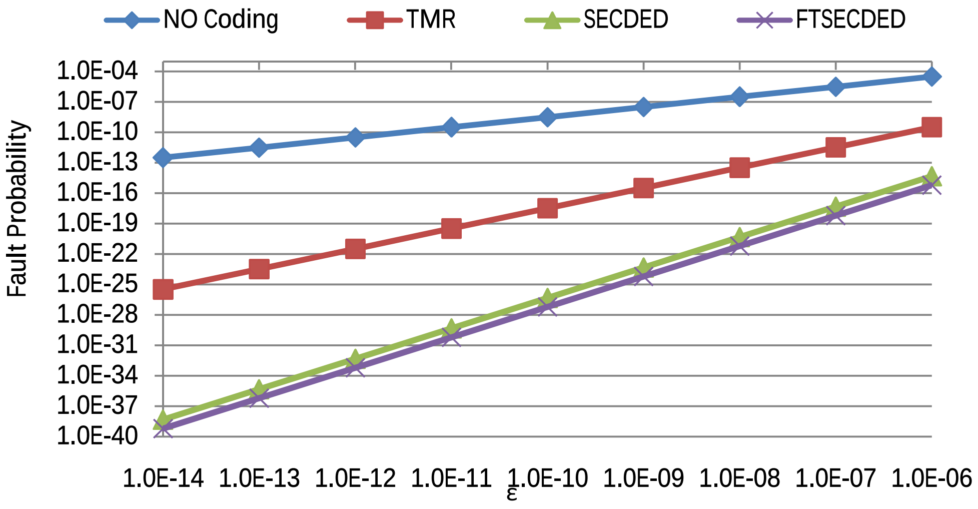

Figure 6. Fault probability of NoCoding, TMR, SECDED, FTSECDEDwith p_n=0

5. Conclusion

We have designed a buffering fault-tolerance router with efficient level and power consumption. In fact, we used free virtual channels to save packets. We implemented virtual channel as two channels to avoid deadlock. Proposed method is implemented by VHDL and evaluated by CAD Tools. The result showed that the proposed method occupies less area and has less power consumption and shorter critical path. In addition, we used analytical model to evaluate fault tolerance. The result of diagram shows improvement of dynamic power consumption, decreasing of occupancy level and error possibility or increasing of reliability.

References

[1] A.P. Frantz, F.L. Kastensmidt, L. Carro, and E. Cota,"Dependable Network-on-Chip Router Able to Simultaneously Tolerate Soft Errors and Crosstalk," Proceedings of the IEEE International Test Conference, pp. 1-9, 2006.

[2] A.P. Frantz, M. Cassel, F.L. Kastensmidt, E. Cota, and L. Carro, "Crosstalk and SEU-Aware Networks on Chips", IEEE Design & Test of Computers, pp.340-350, 2007.

[3] P.T. Huang, W.L.Fang, Y.L. Wang, and W. Hwang, "Low Power and Reliable Interconnection with Self-Corrected Green Coding Scheme for Network-on-Chip," Proceedings of the Second ACM/IEEE International Symposium on Networks-on-Chip, pp. 77-83, 2008.

[4] J. Kim, D. Park, C. Nicopoulos, N. Vijaykrishnan, and C.R. Das, "Design and Analysis of anNoC Architecture from Performance, Reliability and Energy Perspective," Proceedings of the International Symposium on Architecture for Networking and Communication Systems (ANCS'05), pp. 173-182, 2005.

[5] D.Rossi, P.Angelini, C.Metra, "Configurable Error Control Scheme for NoC Signal Integrity," 13th IEEE International On-Line Testing Symposium (IOLTS 2007).

[6] J. Kim, D. Park, C. Nicopoulos, N. Vijaykrishnan, and C.R. Das, "A Low Latency Router Supporting Adaptivity for On-Chip Interconnects," Proceedings of the 42nd Design Automation Conference (DAC'05), pp. 559-564, 2005.

[7] D. Park, C. Nicopoulos, and C.R. Das, "Exploring Fault-Tolerant Network-on-Chip Architectures," Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'06), pp. 93-104, 2006.

[8] M Koibuchi, H. Matsutani, H. Amano, and T.M. Pinkston, "A Lightweight Fault-Tolerant Mechanism for Networks-on-Chip,"Second ACM/IEEE International Symposium Networks-on-Chip, pp.13-22, 2008.

[9] B.Fu, P.Ampadu." On Hamming Product Codes With Type-II Hybrid ARQ for On-Chip Interconnects". IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS.I: REGULAR PAPERS, VOL. 56, NO.9, SEPTEMBER 2009.

[10] M. Pirretti, G.M Link, R.R. Brooks, N. Vijaykrishnan, M. Kandemir, and M.J. Irwin, "Fault Tolerant Algorithms for Network-on-Chip Interconnect," Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI'04), pp. 46-51, 2004.