



AENSI Journals

Journal of Applied Science and Agriculture**ISSN 1816-9112**Journal home page: www.aensiweb.com/jasa/index.html

A method of data encryption in NOC

¹O. Rahmani and ²A. Taherkhani

¹Department of Electrical Engineering, Takestan Branch, Islamic Azad University, Takestan, Iran

²Department of Physics, Faculty of Science, Takestan branch, Islamic Azad University, Takestan, Iran.

ARTICLE INFO

Article history:

Received 20 February 2014

Received in revised form 16

8 April 2014

Accepted 15 April 2014

Available online 5 May 2014

Key words:

Network; Chip, NOC

ABSTRACT

Since today the technology is approaching towards the smaller dimensions; links compared to routers also have a significant role in power loss and energy consumption. In this paper, we aim to reduce power loss and energy consumption in the links and reduce noise by introducing a new technique for data encoding. This technique suggests the reduction in the number of bits and the number of transmissions compared to the original non-encrypted data encryption. Since this is performed in NI, there is no need to make changes in routers' architecture and no significant decrease in area is observed.

© 2014 AENSI Publisher All rights reserved.

To Cite This Article: O. Rahmani and A. Taherkhani., A method of data encryption in NOC. *J. Appl. Sci. & Agric.*, 9(4): 1903-1906, 2014

INTRODUCTION

Continually, need for wider bandwidth is increasing as a result of wider communication links. Also, the technology moves toward the power consumption in wires rather than the logic. Thus, the contribution of power in links is greater than that of the routers (Palesi, M., *et al.*, 2011).

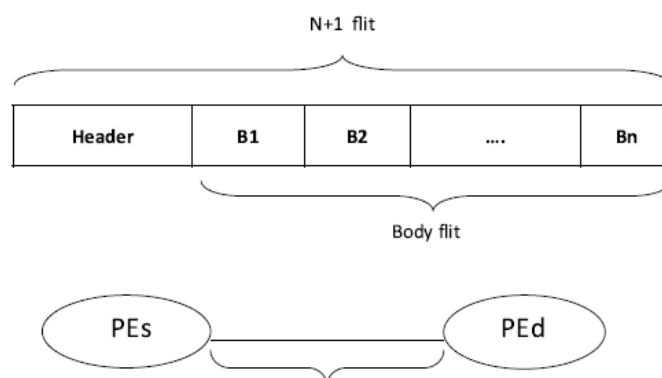
In addition, increase in the number of cores leads to increase in the size of the chip; that is, it will increase the path length. Therefore, we can say that the data coding, is a viable solution for reduction of power consumption. According to the literature (Jabarali Jamali, M., A. Asil.hasil., 2010), it is preferred that the coding and decoding would be performed in NI. It encrypts the NI flits of the main data and header flits in router are added to main data flits. If it is intended to do the encryption after adding the header to the main data, the decryption should be performed after every data is received by routers; thus, it would be able to reach its destination. Therefore, to reduce the power loss in intermediate routers, it is preferred that the header would not be encrypted. Several techniques are introduced to reduce power loss over the links in NOC.

Encoding and decoding have an additional cost that this could be covered through traffic and data transmission rate reduction.

Serial links offer lower bandwidth than the parallel mode and low bandwidth is associated with possible congestion and reduced speed. However, data compression techniques can reduce the number of bits transmitted (Simon Ogg, Bashir Al-Hashimi, 2006).

Quantitative analysis (1):

General model to quantify communication energy savings which allows defining through the use of end to end data encryption.



h, numbers of HOP and h+1, routers

Corresponding Author: O. Rahmani, Department of Electrical Engineering, Takestan Branch, Islamic Azad University, Takestan, Iran
E-mail: o.r.seryasat@tiau.ac.ir

Formulation prior to consideration of encode, decode within the NI:

$$P(pkt) = P_{ni} + P_r + P_{link}$$

$$P(pkt) = 2(n+1)P_{ni} + (h+1)P_{rh} + n(h+1)P_{rb} + h(n+1)P_{link}$$

P_{rh} : The average power loss in a router, when body flits and header flits pass through

P_{ni} : NI average power loss

P_{link} : Average power loss, when a flit passes through the link

P_r : The average power loss in a router

Formulation after the consideration of encode, decode within the NI:

$$P'(pkt) = 2P_{ni} + 2nP'_{ni} + (h+1)P_{rh} + n(h+1)P_{rb} + h(n+1)P'_{link}$$

P'_{ni} : NI power loss when logic code and decode are added to NI

P'_{link} : Power loss, when an encrypted flit passes through the link

$P_{(en/de)}$: Power loss of code and decode. Therefore, P'_{ni} can be written as following:

$$P'_{ni} = P_{ni} + P_{(en/de)}$$

Power reduction percentage after making use of encoder/decoder:

$$PR = \frac{P(pkt) - P'(pkt)}{P(pkt)} = 1 - \frac{P'(pkt)}{P(pkt)}$$

By analysis of the above formula, in the paper (1), they came to conclusion that factors which are effective in reducing power loss during encoding, consists of:

1. Increasing the hopcounts
2. Increasing links' power contribution rather than routers' power contribution
3. Increasing the packet size

That's why we say that the data coding, is a proper way to reduce power consumption.

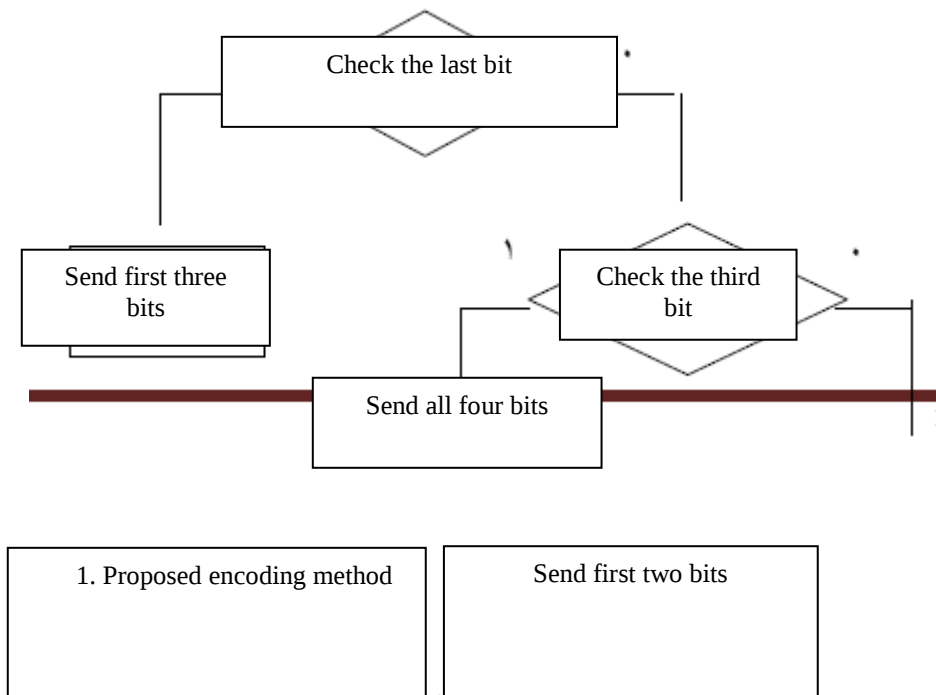
Suggestions for reducing packet size:

Assume link has two bytes (16 bits), transmitting 4 bits of data simultaneously and in parallel, and for each 4-bits, first it leaves the encoder.

What each of the encoders does:

Consider 4 bits, from right or left of the whole data (does not matter) and look at the last bit of it. If it is equal to 1, sends the first 3 bits. If the last bit is 0, the next bit is checked and if it was 0, as well, sends 2 remaining bits, but if it was 1, sends the whole 4 bits. Make Null each of the links having no data, so they will not be affected by noise.

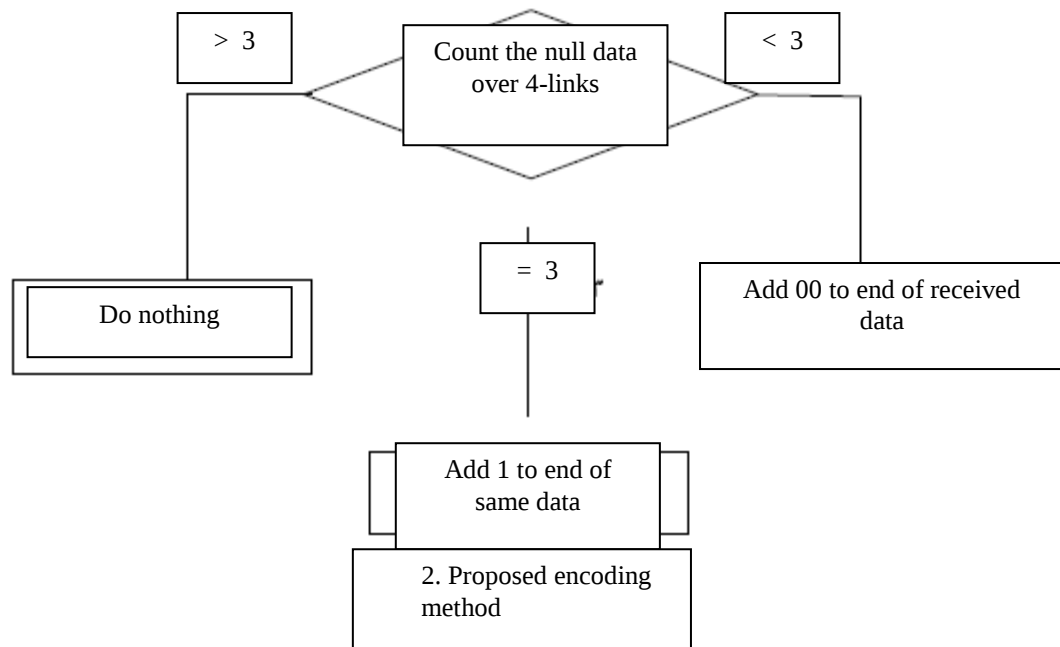
Algorithm that can be considered for encoder:



What each of the decoders does:

It counts the received data, over the 4-links. If it was greater than 3 bits, and the same data, it does not change. If it equals to 3 bits, we add 1 to the final bit. In case of being less than 3 bits, 00 would be added to last 2 bits.

Algorithm that can be considered for encoder:



This operation can either be implemented in hardware or by inserting into a table in the ROM inside the encoder and decoder, in order to search operations, it would be performed in an associative manner.

Example:

Main data

1000/0100/1101/0010

Result of encoding of above data

000/0100/101/10

Result of decoding of the above encoded data

1000/0100/1101/10

This way, you can change the size of the packet that in the best case, the packet length would change to half, and in average case, the packet length would be improved by 25%, and in the worst case, the packet length remains unchanged.

Therefore, this method can be exploited to reduce power loss and noise immunity, without a significant change is observed in the area. Since the encoding and decoding operations are performed in NI rather than in intermediate routers, it leads to improvement of bandwidth usage.

Power of connected wires between two adjacent switches can be described as (Vitkovski, A., *et al.*, 2008).

$$P_{Net} = \frac{1}{2} \alpha C_{Net} V_{DD}^2 f$$

C_{Net} connected wire capacitor and α mean activity of switching on the wire (activity switching, is a defined ratio as the number of bits switched from the $1 \leftarrow 0$ and $0 \leftarrow 1$ to the total number of bits passing through the wire). f , clock frequency and V_{DD} is power supply voltage.

The amount of f , C_{Net} and V_{DD} depend upon the technology process, but data switching activity depends upon the inter-transitions of wires. According to this equation, the power consumption and switching activities have a direct relationship with each other. So we can say that power can be saved, by reducing switching activities. The proposed method reduces the number of bits and therefore is expected to lower the switching activity and consequently, the power consumption.

Conclusions:

Links perform a significant role in power loss (Carlioni, L., *et al.*, 2008; Palma, J.C.S., *et al.*, 2007; Mohammad Ali Jabraeil Jamali). Therefore, in this paper, by introducing a model of encryption and data compression, efforts put to amend the power loss, increase the bandwidth and noise immunity. It would be performed end to end, and intermediate routers do not need to be changed.

Only NI includes encoding/decoding logic; although, it includes an overhead, but it would not be considered as a major problem of cost and time delay. The proposed encryption program, by decreasing size of the packet, reduces contribution of the power.

REFERENCES

- Carlioni, L., A.B. Kahng, S. Muddu, A. Pinto, K. Samadi and P. Sharma, 2008. "Interconnect modelling for improved system-level design optimization," in Proc. AsiaSouthPacificDesignAutom.Conf., pp: 258-264.
- Jabarali Jamali, M., A. Asil.h;asil., 2010. "Presentation of New Method for Reducing Overhead and Increasing Tolerant in Networks on Chip by Data Coding" Australian Journal of Basic and Applied Sciences, 4(10): 4846-4851.
- Mohammad Ali Jabraeil Jamali, Ahmad Khademzadeh, Hasan Asil, and Amir Asil, 2009. "Encoding and Compressing Data for Decreasing Number of Switches in Baseline Networks" World Academy of Science, Engineering and Technology. Pariss., pp: 54.
- Palesi, M., G. Ascia, F. Fazzino, V. Catania, 2011. "Data Encoding Schemes in Networks on Chip," Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, 30(5): 774-786.
- Palma, J.C.S., L.S. Indrusiak, F.G. Moraes, A.G. Ortiz, M. Glesner and R.A.L. Reis, 2007. "Inserting data encoding techniques in to NoC-based systems," in Proc. IEEE Comput. Soc. Annu. Symp. VLSI, pp: 299-304.
- Simon Ogg, Bashir Al-Hashimi, 2006. "Improved Data Compression for Serial Interconnected Network on Chip through Unused Significant Bit Removal," vlsid, pp.525-529, 19th International Conference on VLSI Design held jointly with 5th International Conference on Embedded Systems Design (VLSID'06).
- Vitkovski, A., R. Haukilahti, A. Jantsch, E. Nilsson, 2008. "Low-power and error coding for network-on-chip traffic," IET Comput. Digit. Tech., 2(6): 483-492.