J. Basic. Appl. Sci. Res., 3(2s)62-65, 2013

© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

A Method for Cryptography in Networks on Chip

H. abbasi[1], M. mazaheri[2], M. reshadi[3]

Department of computer, Science and Research Branch, Islamic Azad University, Tehran, Iran

Received: June 10 2013
Accepted: July 10 2013

ABSTRACT

Since today technology is moving toward smaller size, links in comparison to routers have amazing role in power dissipation and power consumption. The goal in this paper is to reduce power dissipation and power consumption in links also reducing noise by introducing a new technique for data encryption. This technique recommends reducing the number of bits and transmissions in comparison to plain text. Because this function happens in NI and it isn't necessary to make changes in the architecture of routers, also you can't see appreciable reduction in the area.

KEYWORDS: Data encoding , low power , network on chip , link

INTRODUCTION

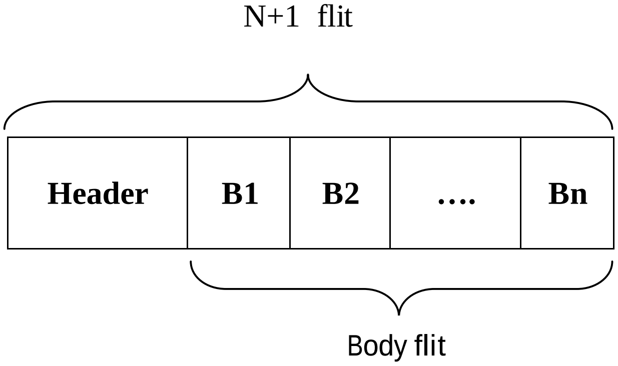
Continuous needs for enhancement of bandwidth and communication links are inevitable. Also technology is moving toward power consumption in links until logic. Therefore portion of power in links are more than portion of power in routers [1].In addition, once the number of IP's increase then chip size will increase which it leads length of path become longer. Therefore we can tell that encoding is a suitable solution for decreasing the power consumption. Now according to the previous works [2] it is preferred that encoding and decoding happen in NI.

NI will do the encryption the main data flits and the header flits in the router join to the main data flits.

If we want to do the encryption after adding header to main data, in this case each time that data arrive to the routers must be done the decryption, in order to reach the final destination. So to decrease power dissipation in middle routers we prefer to don't the encryption header. Few techniques have been introduced for reducing power dissipation on links in NoC. Encryption and decryption have extra cost, however it could be covered by reducing traffic and data transfer rate. Serial links offer less bandwidth in comparison to parallel links also less bandwidth could have possibility of congestion and speed reduction, but we can decrease the number of send bits with compression techniques [4].

Quantitative Analysis [1]:

The general model for quantitative determination of energy saving that could be defined by using end-to-end encryption technique.



Making formula before considering encoding and decoding within NI:

P(pkt) = Pni + Pr + Plink

$P(pkt) = 2(n+1)Pni + (h+1)Prh + n(h+1)Prb + h(n+1)PlinkA$

Prh , Prb: Average power dissipation in router when body and header flits pass from it.

Pni: Average power dissipation in NI.

Plink: Average power dissipation when a flit passes link.

***Corresponding Author:** Haniyeh Abbasi, Department of computer, Science and Research Branch, Islamic Azad University, Tehran Iran. Email:h.abasi24@gmail.com; Mobile:0098-9375022504

Pr: Average power dissipation in router.
Making formula after considering encoding and decoding within NI:

$$P'(pkt) = 2Pni + 2nP'ni + (h+1)Prh + n(h+1)Prb + h(n+1)P'link$$

P’ni: Power dissipation in NI when encoding and decoding logic is added to NI.
P’link: Power dissipation when an encoded flit passes link.
P(en/de): Power dissipation for encoding and decoding, as a result we could write:

$$P'ni = Pni + P(en/de)$$

Percentage of reduction in power dissipation after using encoder and decoder:

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

By analyzing above formulas in paper [1], they concluded what in reduction of power dissipation during encryption is effective including:
1) Increasing Hop counts
2) Increasing portion of link power in comparison to portion of routers power.
3) Increasing size of packet
That is why data encoding is an appropriate way for decreasing power consumption.

An offer for decreasing size of packet:

Suppose our link is 2 byte (16 bits) which it simultaneously sends data in form four bit four bit and parallel.
Function of each encoder:
From left or right the total data (No Matter), consider 4 bit in mind. Look at the last bit, if it was equal to 1 then send first 3 bit. If it was 0, consider next bit and if this one was 0 too then send next 2 remaining bit, but if it was 1 then send all 4 bit. Each one of the links that there is no data on it should become NULL, so it can’t become under the influence of noise.
Algorithmic Model for Encoder:

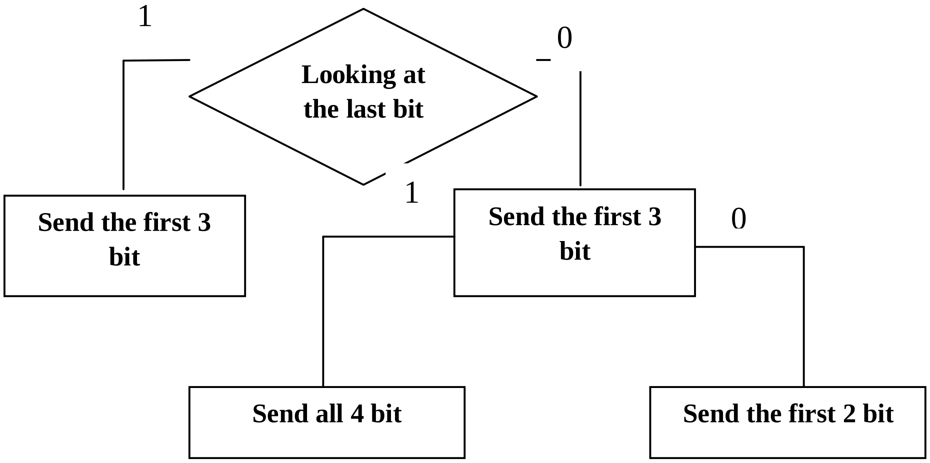


Fig. 1. Offered encoding method

Function of each decoder:
It counts those received data on 4 bit link, if it was more than 3 bit with the same data then it doesn’t change. If it was equal to 3 bit then decoder adds 1 bit to the last. If it was less than 3 bit then is added 00 to the last 2 bit.

Algorithmic Model for Decoder:

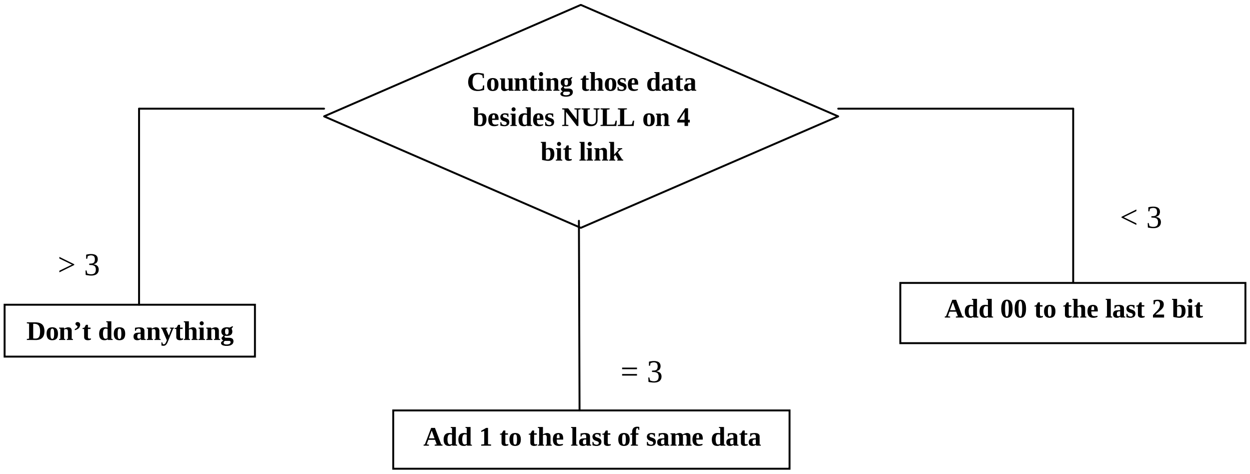

Counting those data besides NULL on 4 bit link
> 3
Don't do anything
= 3
Add 1 to the last of same data
< 3
Add 00 to the last 2 bit

Fig.2. Offered decoding method

It is possible to implement this function either as hardware or to put it in ROM table into encoder and decoder that searching function happens like associative.

Examples:

Main data
1000 / 0100 / 1101 / 0010
Result of encoding over main data
000 / 0100 / 101 / 10
Result of decoding over encoded data
1000 / 0100 / 1101 / 0010

In this way you can make changes in the packet size which in best case packet length becomes half and in average case packet length will improve up to 25% and in worst case packet length doesn't change.

Therefore this method causes reduction of power dissipation and influence of noise without significant changes in area because encoding and decoding happens in NI not in middle routers. Also this will improve usage of bandwidth.

Power of wires connected between vicinal switches can be described by following formula [3]:

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

C_{Net} is capacitor of connected wires and α is average switching activity over wire (the objective of switching activity is a defined ratio of number of switched bits 0 → 1 , 1 → 0 over total bits passing through the wires). f is frequency of clock and V_{DD} is voltage of power source.

Amount of , C_{Net} and V_{DD} depends on process of technology but amount of switching activity depends on data and transmissions amongst wires. According to this formula power consumption and switching activity have a direct relation to each other so we can tell by reducing switching activity we can save the power. Since offered method reduces the number of bits it is expected the switching activity will become less and as a result power consumption will become less too.

Conclusion

Links play important role in power dissipation for NoC [5]-[7]. Therefore in this paper by introducing a cryptography method and data compression it tries to improve power dissipation, increase bandwidth and reduce influence of noise. This action happens like end-to-end and it is no need to create any changes in the middle routers.

Only NI includes encoding / decoding logic. However it carries overhead but it isn’t being considered essential problem in cost and delay. Also this offered cryptography method by reducing packet size reduces portion of power.

REFERENCES

1) Palesi, M.; Ascia, G.; Fazzino, F.; Catania, V., "Data Encoding Schemes in Networks on Chip," Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on , vol.30, no.5, pp.774,786, May 2011

2) Jabarali Jamali.M;Asil.h;asil.A;“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, 2010

3) Vitkovski, A.; Haukilahti, R.; Jantsch, A.; Nilsson, E., "Low-power and error coding for network-on-chip traffic," IET Comput. Digit. Tech., 2008, Vol. 2, No. 6, pp. 483– 492

4) Simon Ogg, Bashir Al-Hashimi, "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), 2006

5)L.Carloni,A.B.Kahng,S.Muddu,A.Pinto,K.Samadi,andP.Sharma,“Interconnect modelling for improved system-level design optimization,” in Proc.AsiaSouthPacificDesignAutom.Conf.,2008,pp.258–264

6)J.C.S.Palma,L.S.Indrusiak,F.G.Moraes,A.G.Ortiz,M.Glesner,andR.A.L.Reis,“Inserting data encoding techniques in to NoC-based systems,”in Proc.IEEEComput.Soc.Annu.Symp.VLSI,Mar.2007,pp.299–304.

7) 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