International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 6, December 2018, pp. 4164~4174
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp4164-4174

Reconfigurable High Performance Secured NoC Design Using Hierarchical Agent-based Monitoring System

Kendaganna Swamy S, Anand Jatti, Uma B. V
Department of Electrical & Communication Engg, R.V College of Engineering, India

Article Info

Article history:

Received Mar 3, 2018
Revised Jul 18, 2018
Accepted Aug 7, 2018

Keyword:

Congestion
Fault identification
Fault tolerant
Network fault
Network-on-chip
Routing

ABSTRACT

With the rapid increase in demand for high performance computing, there is also a significant growth of data communication that leads to leverage the significance of network on chip. This paper proposes a reconfigurable fault tolerant on chip architecture with hierarchical agent based monitoring system for enhancing the performance of network based multiprocessor system on chip against faulty links and nodes. These distributed agents provide healthy status and congestion information of the network. This status information is used for further packet routing in the network with the help of XY routing algorithm. The functionality of Agent is enhanced not only to work as information provider but also to take decision for packet to either pass or stop to the processing element by setting the firewall in order to provide security. Proposed design provides a better performance and area optimization by avoiding deadlock and live lock as compared to existing approaches over network design.

Corresponding Author:

Kendaganna Swamy S,
Department of Electrical & Instumentation,
R.V College of Engineering,
Bangalore, India.
Email: kendagannaswamys@rvce.edu.in

1. INTRODUCTION

Since last 50 years, as a result of advancement in semiconductor technology, scaling continues from today's 16nm feature size to 1nm feature size expected in 2028 [1]. This enables to integrate more number of IP cores in a single system on chip. With the growth of number of cores, communication demand between the processing cores increases. This may require high communication bandwidth with low latency, low power consumption and high scalability network. The conventional bus based architecture will not meet these requirements and this lead to communication performance bottleneck. A solution for such a communication bottleneck is network on chip to improve the performance for many core systems [2]. As compared to previous works presented in [3], [4], NoC is the popular interconnection infrastructure for many core inter communication because of its high throughput, low latency, scalability and reusability. NoCs are composed with three components such as router, links and network interface (NI). Routers are the switching elements that are responsible for forwarding the data packets from one router to another one.

Links are the connection parts between different nodes and they are usually bidirectional network interfaces, which acts as the wrapper between the router and processing elements (PE). Routers will take the routing decision based on the routing algorithm. In NoC based multiple core systems, the negative aspects of technology scaling may increase the probability of chip defects introduced which may be either in operational or in manufacturing phases. These faulty NoC systems may have defects in processing elements (PE) or routers or interconnects. Due to the faulty interconnects and routers, the number of routing paths are reduced, which results in unbalanced traffic distribution and more traffic congestion [5]. The lack of non local fault awareness leads to performance degradation in NoC. The performance parameters are becoming

important aspects in multiple core chip design. In this proposed design the reconfigurable high performance secured NoC design using hierarchical Agent based monitoring system provides a promising solution to address the above issue [6], which is suitable for large multi core systems with hundreds of processing elements. In this design, agents are distributed hierarchically to accumulate, distribute and manage the faulty information along with security using random arbiter router with XY routing algorithm.

The previous works are related to the hierarchical agents found in [7]-[11]. In [6] and [11] the overall structure of agent based management system is discussed without any detailed design. The hierarchical agents are used in [8] and [7] to monitor the power consumption in NoC using DVFS (differential voltage and frequency scaling) technique. In [10] an agent based management method is used to enhance the performance of NoC based multi core system on chip design against the faults or failures resulted in the neighbor nodes in addition to their own components and interconnection links. These agents inform the routers about different faults in the network which helps the routing process to be more scalable using XY routing algorithm and also to improve the performance. However, still many issues need to be addressed. Previous works are limited to 4x4 agent based NoC, non reconfigurable and non secured agents. The arbiters used in the previous router are not servicing the packets equally in all directions of the node and it serves the packet according to the priority which may lead to increase in packet staking in one direction. The agent provides only the congestion and healthy status of the network.

In the proposed design all these limitations are addressed, by introducing reconfigurable NxN hierarchical agent based NoC with random arbiter router using XY routing algorithm, which overcomes the packet stacking by servicing the packet randomly, which avoids loss of packets and improves the memory area. The agent functionality is further enhanced to work as an information provider and also take decision for packets to either pass or stop to the processing element by setting the firewall which intern provides security. Section 1.1 discusses about the existing literatures where different techniques are discussed for detection schemes used in power transmission lines followed by discussion of research problems in Section 1.2 and proposed solution in 1.3. Section 2 discusses about algorithm implementation followed by discussion of result analysis in Section 3. Finally, the conclusive remarks are provided in Section 4.

1.1. Background

This section discusses about the existing approaches for solving the identification problems of network related faults. The work carried out by Santos et al. [12] has presented a mechanism to identify maximizd impedence faults using discrete wavelet transform. Study toward identification of real-time faults has also been carried out by Pignati et al. [13] over similar distributed network using state-based estimation technique. Similar form of approach was also implemented by Nikander and Jarventausta [14] for network fault identification. Considering a case study of spacecraft, Raiteri and Portinale [15] have used Bayesian network for identifying and mitigating faults occurring over spacecraft. Research towards explicit analysis of behaviour of a packet is carried out by Wang et al. [16] using a unique form of classification technique. Adoption of probability theory has been used for developing a framework for identifying faults over sensory application as witnessed in the work of Ntalampiras [17].

The authors have used Hidden Markov Model for this purpose. Zhang and Zhang [18] have used graph-based approach for developing a framework of fault identification taking the case study of satellite network. The occurances of network fault is also investigated over an optical network by Amaral et al. [19] where the authors have used specific device to accomplish the task. Similar study towards optical network has been also studied by Zhu et al. [20], where a mathematical modeling has been utilized for developing two dimensional coding-monitoring systems. Adoption of Bayesian network is again seen for the work carried out by Cai et al. [21]. There have been also studies towards developing fault tolerance system in existing literature. Considering the case study of chip switching, Kohler et al. [22] have developed an fault tolerant model for improving Network-on-chip performance. Vall et al. [23] have developed an estimation technique of faults occurring in sensory network.

Yao et al. [24] have linear state feedback mechanism for developing a controller system of significant faults occurring over network architecture. Eghbal et al. [25] have carried out anlaysis of network-on-chip architecture for overcoming various hardware related issues on chip design. Ren et al. [26] have presented an adaptive communication strategy to overcome faults for mitigating deadlock condition. Shuwaili et al. [27] have discussed about fault tolerance mechanism for network function virtualization using coding-based approach. Similarly Pereira et al. [28] and Wu et al. [29] have also presented a mechanism of fault tolerance system for chip and sensor nodes respectively. Therefore, it can be seen that there are various reserahers who have already carried out studies towards improving the performance of fault tolerance associated with the network system especially the chip-based architecture. Each approach has their own uniqueness as well as limitation. The next section outlines the problems associated with the existing research.

1.2. Research Problem

The significant research problems are as follows:

a. Existing research towards fault tolerance doesn't emphasize on the scalability while evolving up with fault tolerant protocol over network design.
b. None of the existing studies towards NoC has highlighted any design issues with its processing elements that offer latent faults in any network architecture.
c. Although existing studies have worked on fault identification but there are less number of studies towards classifying the faults existing over the networks.
d. The mechanism of formulating the decision in ensuring better performance of fault tolerance network is not clearly defined in any existing studies.

Therefore, the problem statement of the proposed study can be stated as "Developing a cost effective modeling to encapsule comprehensive network faults with equivalent focus on packet-level controlling mechanism in chip architecture is computationally challenging."

1.3. Proposed Solution

The prime aim of the proposed system is to develop a simple and novel approach that can optimize the performance of the network by performing integrated operations over the network. With an aid of an analytical modeling, the proposed system performs a series of operation e.g. i) identification of faults, ii) identification of traffic bottleneck conditions, iii) incorporating pacey-level security, and iv) effective monitoring of the ongoing communication. The proposed system acts like a complimentary model to assists the router for formulating a precise decision. The schema of the proposed system is as shown in Figure 1.

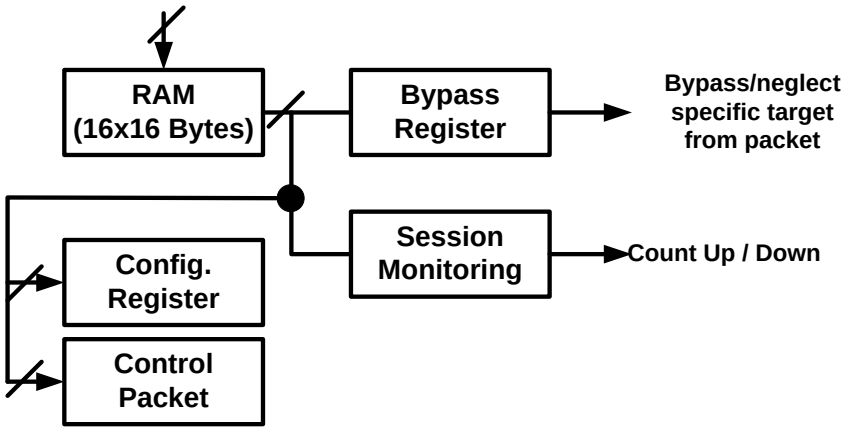

Figure 1. Schema of Proposed Method

The proposed scheme assists in aggregating, managing, and distributing the information related to network faults using Local Fault Register (LFR) while it takes the help of Regional Fault Register (RFR) for performing updating operation on its neighboring nodes. The cell agent exchanges the congestion information bidirectional between the agents by using same link inside the dedicated network [30]. The congestion information or the fault information is determined by the agents with the help of encoding and decoding process. This cell agent will provide the security to the processing element using config register and control packet stage. Config register is used for source port configuration (using lookup table concept) in order to block the unwanted and unrelated packets to give security (like blocking the website or virus packets). Control packet will get the authorized packet information from the config register and decides whether packet must be passed or not to the processing element. In general, people can hack the secured firewall, but in the proposed design, some of the port addresses are itself blocked in the hardware (i.e inside the chip), which avoids the intruder by hacking the firewall. The cell agent will ignore or bypass some of the packets, if those packets contain video or audio related data using bypass register. The agents will also monitor the maximum sessions per node using session monitoring stage. This session monitoring stage will take care of start session and close session (limited to 0-31 sessions) after performing the task. The next section outlines about the algorithm used for this purpose.

2. ALGORITHM IMPLEMENTATION

This information related to the fault in the network is quite useful for the router to formulate an effective decision making during routing. The fault detection circuitry in the agent will provide the fault information of the network. A NoC router is assumed to contain a priority encoder, random arbiter and the crossbar switch. As compared to technique in existing system [10], [31], [32], in this paper the proposed router design buffers are avoided to reduce the hardware overhead and to improve the performance. The priority encoder which selects the inputs according to the select signal originates from the random arbiter. This proposed router will serve the packets randomly without any loss or stacking of the packets. With reference to [7], [33] fault detection circuitry is adopted in the NoC router and the links are used to detect the permanent faults on the network with an acceptable hardware overhead.

The fault detection circuitry will provide the appropriate signals, which gives the information of fault awareness related to random arbiter, priority encoder, crossbar switch and all links in four direction of each router. In addition to this, it also provides information of faultiness of other components such as Processing Element (PE) or core and Network Interface (NI). In the proposed design, all the links of the network are bidirectional and if any permanent fault occurs in any one direction, then the entire link will be treated as faulty. Assume a south direction router is faulty or unavailable for routing process, only if the south link or south input pin of the current node or the north input pin of the south neighbor router is faulty. This condition is stated in equation (1) using fault detection stage generated signal.

$$S=Link_s \text{ or } In\_Port_S^{Current\_router} \text{ or } In\_Port_N^{S\_Router} \quad (1)$$

In equation (1) all the terms are one bit status, if any term is equal to '1' then respective component is faulty, else it is healthy. In any router if the input pin is faulty then it can be modeled by assuming its link is faulty. equation (2) is basically used for all the four directions of the router.

$$n=Link_n \text{ or } In\_Port_n^{Cur\_Router} \text{ or } In\_Port_{(1-n)}^{n\_router} \quad (2)$$

In (2) 'n' can be a E, W, N or S i.e East, West, North or South directions, respectively. $Link_n$ shows the status of current router i.e bidirectional link in the 'n' direction. $In\_Port_n^{Cur\_Router}$ gives the status of the input pins of priority encoder in the 'n' direction of the current router and $In\_Port_{(1-n)}^{n\_router}$ gives the status of neighbor router input port to which the opposite direction of n and placed in the n direction of the current router. (1-n) indicates the opposite direction of n, which means N, S, E and W for S, N, W and E directions, respectively. If any one of the component inside the router is faulty, then entire router is considered as faulty. Once the router is faulty it is not available to do its task (i.e routing the packets from input to its corresponding output port). One bit information of LFR is used to indicate the faultiness of the node which is labeled as Node. equation (3) determines the status of the Node/Router.

$$Node=Priority\_encoder \text{ or } Random\_arbiter \text{ or } Crossbar\_Switch \quad (3)$$

In equation (3) if any one of the above term is faulty, then entire node is considered as faulty node. In multiple core networks on chip, the processing elements are connected to network via the network interface. If the PE is not working then platform level will automatically remap that packet into some other core on the network according to healthy status information. Equation (4) says that if PE is '1' then it is considered as faulty or its network interface or the local link is connected between the router and PE is faulty then PE becomes unavailable.

$$PE = PE_{Local} \text{ or } NI \text{ or } Link_{Local} \quad (4)$$

Fault informations are determined using equation (1) to (4), which is useful for routing process in order to improve the performance by avoiding dead lock and live lock situation. This fault information is classified and transferred to the top level of the system to map the packet into the healthy node which in turn improves the fault tolerant capability and the cost of routing algorithm [34]. Such local fault information is stored in the LFR. The local fault register is 8 bit in size. In this 6 bits are used for indicating the faulty status and 2 bits for future enhancement. Further in these six bits, the LFR uses four bits to update the status of four input pins of the router, which helps neighbor nodes to update their local fault registers according to equation (2). The remaining 2 bits are used to update the status of Node and PE. Assume that center node is the current node and it is having four neighboring nodes.

The current node updates its own component fault information in LFR and also updates the neighboring fault information with the help of RFR. The RFR is 8 bit in size, in this four bit is used to update

the neighbor node fault information and remaining four bits are used for future enhancement. Equations (1) to (4) will update the LFR of all the nodes. This LFR will help to update the RFR of the entire neighboring node with new faulty information. Accordingly the center node will have the faulty information of N, E, W and S sides of the nodes. If any one bit of LFR of the north side node is equal to one, then the current node RFR will updates the *'NN'* bit to one and the remaining bits will be equal to zero, which says that the north side node is unhealthy and the packets should not be sent towards north node if the destination is top right node.

The proposed hierarchical agent structure is as shown in Figure 2. Each and every cell, cluster agent gets updated with new fault information of its own cluster cell and the neighboring cluster cells bidirectionaly [6]. Such fault information is sent to the top level of the system, which help to map the packet to healthy node by selecting best path. Cluster Separation Module (CSM) helps the packet to reach its respective cluster agent by considering cluster selection bits on the packet. Then the cluster will route the packet into the respective cell agent according to the routing information in the packet. Finally agent will decide whether the packet has to pass or stop into the processing element by providing the security in the agent.

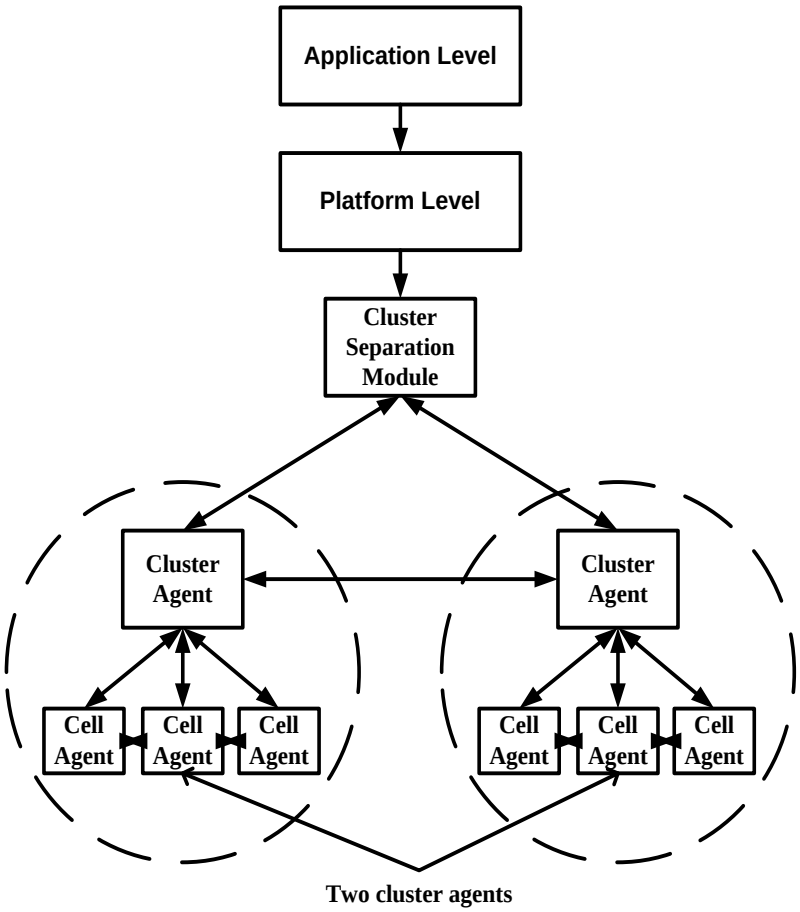

Figure 2. Hierarchical agents in two neighbor clusters

A 4X4 agent based NoC as shown in Figure 3 includes processing element, network interface, router and agents (these agent can be ether a cell agent or a cluster agent). All the agents are connected bidirectionally and one bit information is exchanged between the agents to update the RFR. Later these agents are connected to the NoC router network. Packets from the application level enter into the router via the agents in order to check the security aspects which will be explained in further section. The proposed agent based monitoring system uses two types of communication: namely peer to peer communication (used between the agents) and base line data network communication (for controlling and routing the packets in the network).

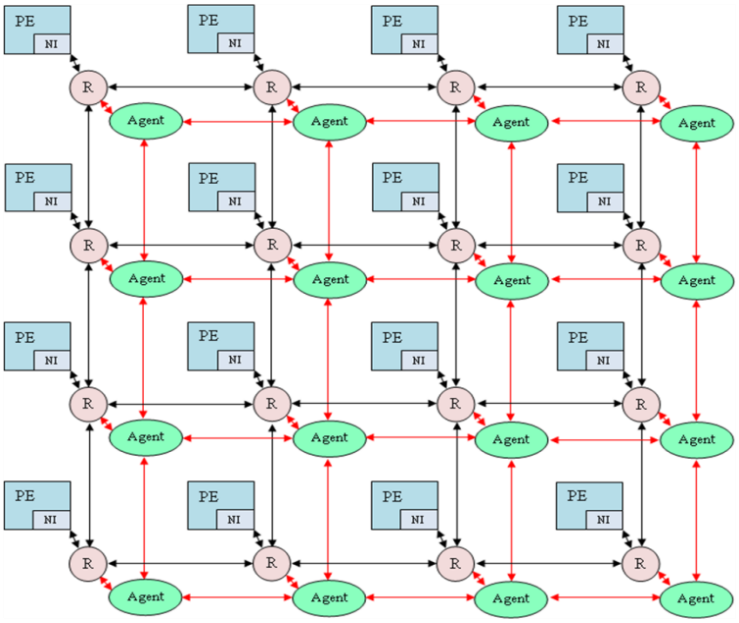

Figure 3. A 4X4 agent based NoC

The cluster agent will accumulate the critical fault information (PE or whole node failure) occurred inside the cluster and will send that information to higher level. Then the cluster will receive the command from the higher level for reconfiguration or remapping of the packet or task migration. The cluster separation module will play an important role to separate the received packet and send it to the respective cluster according to the n^{th} bit of the packet. If the n^{th} bit is zero then the received packet belongs to cluster_1 else it belongs to cluster_2. If the number of clusters increases then the number of cluster selection control bits must also be increased in order to segregates the packet to desired cluster.

The XY based fault tolerant routing algorithm [33],[34] is incorporated in the proposed hierarchical agent based management method. This node is developed based on above discussed mathematical equation. This routing algorithm is low cost, adaptive and congestion aware which is suitable for NoC based multiple core system on chip. For example consider a 3x3 network in which the center node includes the cluster agent. In such network top left node is source node and bottom right is the destination node. The source node should be aware of the status of E, S, ES and SE labeled links surrounded by destination node [35],[36]. The faulty statuses of these links are not updated in the neighbor node of the source node. Then cluster agent will provide this information to the routing algorithm. With the help of this information, the routing algorithm will collectively gather all the faulty and congestion information and reach the desired location in the shortest path. Algorithm (1) shows the management algorithm used by the Hierarchical Agents.

Agent Management Algorithm
Input: Faulty, congestion and security information from cell agents (NA) and neighbor cluster agents (CA)
for each agent **do**
Wait until a new congestion or fault information is received;
If (a node failure **or** NI fails **or** PE fails **or** no control packet is received from a NA within the time) **then**
inform the top level and its associated node agents;
receive the packet remapping or task reallocation information;
segregate the failed PE or Node;
else if (new fault information received from a CA) **then**
inform the new fault and congestion information to neighboring cluster agents and associated node agents;
else if (new fault information from the NA) **then**
inform the new congestion and fault information to neighboring node agents within the cluster agent;

end if
if(destination address of XY == current address of XY) **then**
check the security to decide whether packet has to pass into the destination PE or not;
if(security check = =0) **then**
32 bit packet data will reach the destination Node;
else packet will be discard;
end if

3. RESULT ANALYSIS

To analyze the importance of the proposed hierarchical secured agent based monitoring system on network performance. The 4x4 agent based NoC design using HDL code and simulated using Xilinx ISE 14.2 tool with ModelSim 6.3f respectively. It is synthesized and implemented on vertex 5 FPGA (XC5vFX70T) kit. The performance of proposed method of secured agent based monitoring system is analyzed and compared with the existing methods. In the proposed design each cluster is a 4X4 sub network; in this the center node is treated as cluster agent. It is assumed that 6.25% of faulty node (one node is faulty out of 16 nodes) and 20.83% of faulty link (five faulty links out of 24 links) leads to 27% of system fault is as depicted in Figure 4(a).

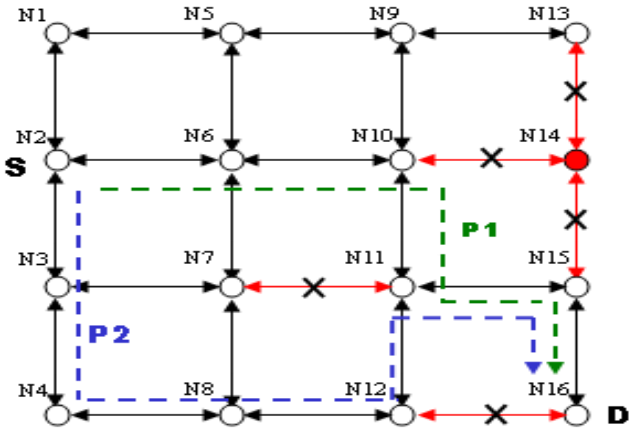

Figure 4(a). A faulty 4x4 NoC

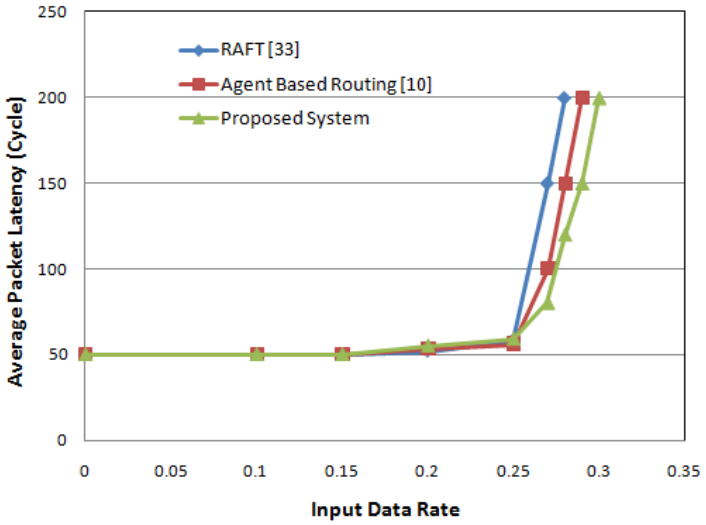

Figure 4(b). Average packet latency analysis

Similar assumption is made for both with and without agent based network and the performance analysis is as shown in Figure 4(a). From the graph it is observed that, a without agent based XY method does not have any means to reliably send all the packets to their destination in the faulty situations, there may be chance of packet stuck in the faulty node then packet has to be resent from the top level, which leads to performance degradation [33]. In the proposed design with the prior knowledge of all the faulty links and nodes the packet will reach the healthy node with a reliable time.

The proposed secured hierarchical agent-based system leads to higher performance and saturation points as compared to method introduced in [10]. As depicted in Figure 4(a) source node S sends the packet to destination node D. In order to reach the packet from source node to destination node there are two paths P1 and P2, among these P1 is the minimal path when compared to P2. However proposed hierarchical secured agent will select the minimal path P1 to route the packet using XY routing algorithm. Figure 5 waveform shows the node to node packet transfer path between node 2 to node 16 (i.e. N2-N6-N10-N15-N16) as highlighted on the waveform. It is synthesized and implemented on vertex 5 FPGA (XC5vFX70T) kit.

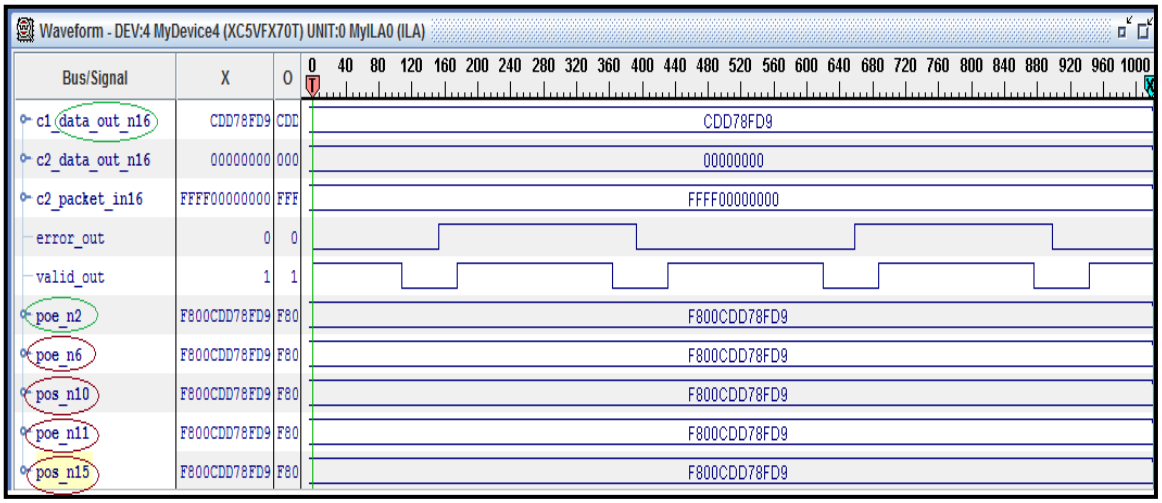

Figure 5. 4X4 secured agent based NoC Design implementation waveform

Figure 6(a) and Figure 6(b) the proposed design throughput is compared with the existing functional diagnosis method with normal and heavy load condition under the uniform traffic. According to the graph, the proposed method has high throughput as compared to the method introduced in [30]. To analyze the area overhead of the proposed design, the implemented DyXY [35] is the basic adaptive routing method, an adaptive fault tolerant technique RAFT [33], existing Agent based fault tolerant routing algorithm [10] is compared with the proposed secured agent based fault tolerant routing algorithm using HDL code with a 201.74 MHz clock speed.

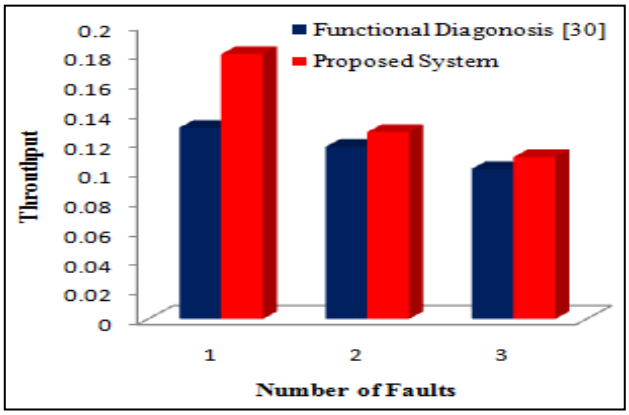

Figure 6(a). Throughput with normal load

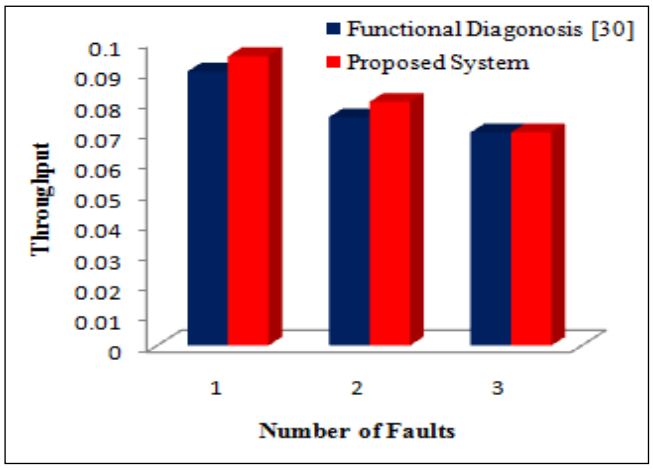

Figure 6(b). Throughput with heavy load

Table 1 shows the area utilization of proposed five port router compared to other existing methods. In addition to this, the table gives the proposed design area overhead as compared to other methods. Based on the hardware analysis table the proposed design area utilization and hardware overhead is 1.4 % improved as compared to existing agent based fault tolerant method [10]. It is worth to mention DyXY method doesn't have reliability to transfer all the packets successfully to their destination under the faulty situation

Table 1. Device Utilization Summary

Routing Method	Area utilization (Gate count) for 5 Port	Area Overhead Comparison (%)
DyXY [35]	36350	12.7
RAFT [33]	39355	4.1
Agent based Routing [10]	41574	NA
Proposed System	40922	1.4

4. CONCLUSION

In this paper, a hierarchical secured agent based monitoring system is proposed for fault tolerant multi core NoC based system on chip. The hierarchically distributed agent will collect, manage and distribute the fault and congestion information of the network to higher level of the system. This fault information helps application level to route the packet to healthy node, which will improve the performance of the network by avoiding the packet latency against faulty node and links. In addition to this the agent will provide security to the PE in order to block the unwanted and unrelated packet entering into the PE which will avoid the live lock situation of the high priority packet which is related to the dedicated node. According to the simulation and synthesis result, the proposed design will enhance the network performance with an improved hardware overhead by using the modified router design.

REFERENCES

[1] International Technology Roadmap for Semiconductors, 2015. Available: http://www.itrs.net/.
[2] W. Dally and B. Towles, "Route packets, not wires: On-chip interconnection networks," *Proc. Des. Autom. Conf.*, pp. 684–689, 2001.
[3] A. Jantsch and H. Tenhunen, "Network on Chip," Kluwer Academic Publishers, 2003.
[4] T. C. Xu, *et al.*, "An optimized network-on chip design for data parallel FFT," *Procedia Engineering*, vol. 30, pp. 313–318,2012
[5] Y. Y. Chen, *et al.*, "Path-Diversity-Aware Fault-Tolerant Routing Algorithm for Network-on-Chip Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol/issue: 28(3), 2017.
[6] M. Valinataj, *et al.*, "Reliable On-Chip Network Design Using an Agent-based Management Method," *Proceedings of the 19th International Conference Mixed Design of Integrated Circuits and Systems (MIXDES)*, pp. 447-451, 2012.
[7] L. Guang, *et al.*, "Hierarchical agent monitoring design approach towards self-aware parallel systems-on-chip," *ACM Trans. on Embedded Computing Systems*, vol/issue: 9(3), 2010.

[8] L. Guang, *et al.*, "Hierarchical power monitoring on NoC - a case study for hierarchical agent monitoring design approach," *Proc. 28th NORCHIP Conf.*, 2010.
[9] P. Rantala, *et al.*, "Novel agent-based management for fault-tolerance in network-on-chip," *Proc. 10th Euromicro Conf. on Digital System Design (DSD)*, pp. 551– 555, 2007.
[10] M. Valinataj, *et al.*, "Enhanced Fault-Tolerant Network-on-Chip Architecture Using Hierarchical Agents," *16th International Symposium on Design and Diagnostics of Electronic Circuits & Systems*, pp. 141-146, 2013.
[11] A. W. Yin, *et al.*, "Hierarchical agent monitoring NoCs: a design methodology with scalability and variability," *Proc. 26th NORCHIP Conf.*, pp. 202–207, 2008.
[12] W. C. Santos, *et al.*, "High-Impedance Fault Identification on Distribution Networks," *IEEE Transactions on Power Delivery*, vol/issue: 32(1), pp. 23-32, 2017.
[13] M. Pignati, *et al.*, "Fault Detection and Faulted Line Identification in Active Distribution Networks Using Synchrophasors-Based Real-Time State Estimation," *IEEE Transactions on Power Delivery*, vol/issue: 32(1), pp. 381-392, 2017.
[14] A. Nikander and P. Järventausta, "Identification of High-Impedance Earth Faults in Neutral Isolated or Compensated MV Networks," *IEEE Transactions on Power Delivery*, vol/issue: 32(3), pp. 1187-1195, 2017.
[15] D. C. Raiteri and L. Portinale, "Dynamic Bayesian Networks for Fault Detection, Identification, and Recovery in Autonomous Spacecraft," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol/issue: 45(1), pp. 13-24, 2015.
[16] H. Wang, *et al.*, "Practical Network-Wide Packet Behavior Identification by AP Classifier," *IEEE/ACM Transactions on Networking*, vol/issue: 25(5), pp. 2886-2899, 2017.
[17] S. Ntalampiras, "Fault Identification in Distributed Sensor Networks Based on Universal Probabilistic Modeling," *IEEE Transactions on Neural Networks and Learning Systems*, vol/issue: 26(9), pp. 1939-1949, 2015.
[18] X. Zhang and Z. Zhang, "Link fault identification using dependent failure in wireless communication networks," *Electronics Letters*, vol/issue: 52(2), pp. 163-165, 2016.
[19] G. C. Amaral, *et al.*, "Automatic Fault Detection in WDM-PON With Tunable Photon Counting OTDR," *Journal of Lightwave Technology*, vol/issue: 33(24), pp. 5025-5031, 2015.
[20] M. Zhu, *et al.*, "Optimal fiber link fault decision for optical 2D coding-monitoring scheme in passive optical networks," *IEEE/OSA Journal of Optical Communications and Networking*, vol/issue: 8(3), pp. 137-147, 2016.
[21] B. Cai, *et al.*, "Bayesian Networks in Fault Diagnosis," *IEEE Transactions on Industrial Informatics*, vol/issue: 13(5), pp. 2227-2240, 2017.
[22] A. Kohler, *et al.*, "Fault Tolerant Network on Chip Switching With Graceful Performance Degradation," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol/issue: 29(6), pp. 883-896, 2010.
[23] E. O. A. Vall, *et al.*, "Distributed Fault-Tolerance for Event Detection Using Heterogeneous Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol/issue: 11(12), pp. 1994-2007, 2012.
[24] J. Yao, *et al.*, "NetSimplex: Controller Fault Tolerance Architecture in Networked Control Systems," *IEEE Transactions on Industrial Informatics*, vol/issue: 9(1), pp. 346-356, 2013.
[25] A. Eghbal, *et al.*, "Analytical Fault Tolerance Assessment and Metrics for TSV-Based 3D Network-on-Chip," *IEEE Transactions on Computers*, vol/issue: 64(12), pp. 3591-3604, 2015.
[26] P. Ren, *et al.*, "A Deadlock-Free and Connectivity-Guaranteed Methodology for Achieving Fault-Tolerance in On-Chip Networks," *IEEE Transactions on Computers*, vol/issue: 65(2), pp. 353-366, 2016.
[27] A. Al-Shuwaili, *et al.*, "Coded Network Function Virtualization: Fault Tolerance via In-Network Coding," *IEEE Wireless Communications Letters*, vol/issue: 5(6), pp. 644-647, 2016.
[28] T. F. Pereira, *et al.*, "Mechanisms to Provide Fault Tolerance to a Network-on-Chip," *IEEE Latin America Transactions*, vol/issue: 15(6), pp. 1034-1042, 2017.
[29] Y. C. Wu and C. C. Tuan, "Fault tolerance events ordering by aging learning in wireless sensor and actuator networks," *IET Communications*, vol/issue: 11(12), pp. 1895-1902, 2017.
[30] G. Schley, *et al.*, "Multi-Layer Diagnosis for Fault-Tolerant Networks-on-Chip," *IEEE Transactions on Computers*, vol/issue: 66(5), 2017.
[31] G. S. N. Ra, *et al.*, "Dynamic Time Slice Calculation for Round Robin Process Scheduling Using NOC," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 5(6), pp. 1480-1485, 2015.
[32] A. H. Brata, *et al.*, "Software Development of Automatic Data Collector for Bus Route Planning System," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 5(1), pp. 150-157, 2015.
[33] M. Valinataj, *et al.*, "A reconfigurable and adaptive routing method for fault-tolerant meshbased networks-on-chip," Elsevier, *Int. J. Electronics and Communications (AEÜ)*, vol/issue: 65(7), pp. 630–640, 2011.
[34] M. Valinataj, *et al.*, "Fault-aware and reconfigurable routing algorithms for Networks-on-Chip," *IETE Journal of Research*, vol/issue: 57(3), pp. 215–223, 2011.
[35] M. Li, *et al.*, "DyXY- a proximity congestion-aware deadlock-free dynamic routing method for Network on Chip," *Proc.43th Design Automation Conference (DAC)*, pp. 849–852, 2006.
[36] Anala M. R., *et al.*, "Performance Analysis of Mesh-based NoC's on Routing Algorithms," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 8(5), 2018.

BIOGRAPHIES OF AUTHORS

Prof. Kendaganna Swamy. S, Assistant Professor Department of Electronics and Instrumentation engineering, R.V College of engineering, Bangalore. He is having 6yrs of teaching experience and 2 years of industry; Area of interest VLSI design, FPGA and NoC. He is published 19 papers along with one national level patent published.

Dr. Uma B.V, working as Professor & Head in Department of electronics and communication engineering, R.V College of engineering, Bangalore. She is having 25yrs of teaching experience, Area of interest VHDL, VLSI design, Digital Electronics Circuits, Synthesis and optimization of digital circuits, CAD tools for VLSI, CMOS VLSI design. She is published 48 papers.

Dr. Anand Jatti, working as an Associate Professor Department of electronics and instrumentation engineering, R.V College of engineering, Bangalore. He is having 14yrs of teaching experience; Area of interest image processing, signal processing and VLSI .He is published 23 papers.