ANALYSIS OF STATUS DATA UPDATE IN DYNAMICALLY CLUSTERED NETWORK-ON-CHIP MONITORING

Ville Rantala
Turku Centre for Computer Science (TUCS), Joukahaisenkatu 3-5 B, FI-20520 Turku, Finland
University of Turku, Department of Information Technology, Turku, Finland

Teijo Lehtonen, Pasi Liljeberg, Juha Plosila
University of Turku, Department of Information Technology, Turku, Finland

Keywords: Network-on-Chip, Monitoring, Traffic management, Dynamic cluster, Status update.

Abstract: Monitoring and diagnostic systems are required in modern Network-on-Chip implementations to assure high performance and reliability. In this paper a dynamically clustered NoC monitoring structure for traffic monitoring is presented and issues concerning status data update intervals have been analyzed. The results show that status update interval protocol has influence to the overall performance.

1 INTRODUCTION

Network-on-Chip (NoC) based systems require versatile monitoring systems to handle the functionality and maintain their performance. The monitoring systems are becoming a more significant part of modern NoC systems. An advantage of the NoC paradigm is its scalability (Dally and Towles, 2001). A fully scalable NoC architecture should have a scalable monitoring system which can be easily tailored to different NoC implementations and whose performance is not degraded when the size of the system increases.

Traffic management is implemented into NoC systems to maintain network performance and functionality in the case of faults and under high traffic load. There is a monitoring system to collect traffic information from the network and adaptive routing which can be reconfigured when the circumstances in the network change. Two types of information are required in traffic management: traffic status and locations of faults. Traffic status can be observed from different network components while fault information can cover the faultiness of different network components. Fault information can be simplified by using only the information of faulty links and representing other faulty components by marking the links around these components to be faulty.

A dynamically clustered monitoring structure for NoC is presented and its status update features are discussed in this paper. It is a fully scalable monitoring system which is primarily aimed for traffic management purposes. The paper is organized as follows. Different monitoring structures are discussed in Section 2 and the dynamically clustered monitoring structure is presented and analyzed in Section 3. Finally conclusions are drawn and the future work is discussed in Section 4.

2 MONITORING STRUCTURES

The components of a monitoring system are monitors and probes. The probes are attached to the network components to observe their functionality. The observed data is delivered from probes to a monitor which can collect statistics or process the data to a format which can be utilized in different reconfiguration tasks. The processed monitoring data is finally delivered to the components which use it to reconfigure their operation. In our research we focus on shared-resource structures which require minimum amount of additional resources. In shared-resource structures non-intrusive operation of the monitoring system is a significant issue.

Monitoring structure defines the number and type of monitors and probes, their placing, connections and tasks. A centralized monitoring structure has one

Rantala V., Lehtonen T., Liljeberg P. and Plosila J..
ANALYSIS OF STATUS DATA UPDATE IN DYNAMICALLY CLUSTERED NETWORK-ON-CHIP MONITORING.
DOI: 10.5220/0003359204930497
In *Proceedings of the 1st International Conference on Pervasive and Embedded Computing and Communication Systems* (PECCS-2011), pages 493-497
ISBN: 978-989-8425-48-5

central monitor and several probes that observe the data and deliver it to the monitor. In centralized structure the central monitor has complete overall knowledge of the network but it causes significant amount of monitoring related traffic in the network. A centralized congestion control system is presented in (van den Brand et al., 2007) while a centralized transaction monitoring is implemented in (Ciordas et al., 2006). Centralized NoC monitoring structures are also discussed for instance in (Nollet et al., 2004) and (Mouhoub and Hammami, 2006).

A clustered monitoring structure has a few cluster monitors and several probes. The network is divided into subnetworks, clusters, each of them having a cluster monitor and several probes. The complete network knowledge can be reached using inter-cluster communication but most of the tasks can be realized inside a cluster. However, a clustered structure still causes a considerable amount of monitoring traffic. (Rantala et al., 2011) Clustered monitoring structures have been discussed for instance in (Al Faruque et al., 2008) and (Marescaux et al., 2005).

In an NoC the data is typically transferred as packets which have a destination address. Routers forward these packets based on this address and the applied routing algorithm. (Dally and Towles, 2004) The NoC monitoring systems which use shared communication resources transfer the network status data using monitoring packets. When centralized or clustered monitoring structures are used, these packets have to be routed from probes to a monitor and from the monitor to the routers. Centralized control has its strengths and it is required for several tasks. However to optimize performance some of the traffic management tasks could be executed with simpler distributed, or dynamically clustered, monitoring structure to decrease the load of the centralized control system. (Rantala et al., 2011)

3 DCM STRUCTURE

Dynamically clustered monitoring (*DCM*) does not require any centralized control. There is a simple monitor and a probe attached to each router in the network. Instead of centralized control the monitors exchange information with each other. Each router has a dynamic cluster around itself from where a router collects the data it needs for traffic management and to where the status of the router diffuses. The dynamic clusters of different routers overlap with each other. The simplest dynamic cluster includes four closest neighbors of a router but it can be expanded to neighbors' neighbors and so on. A system which uses DCM for traffic management could have for instance operating system level control for tasks that need complete knowledge of the system. However, when traffic management is implemented with a DCM structure the load of the network can be optimized. (Rantala et al., 2011)

This section is structured as follows. The used simulation environment is presented in Section 3.1. The format of the network status data and the monitoring communication are briefly discussed is Section 3.2. Status data update interval procedures are presented and analyzed in Section 3.3 and Section 3.4, respectively.

3.1 Simulation Environment

A mesh NoC with 100 cores and DCM structure with cluster size of five was simulated and analyzed using a *SystemC* based NoC model. Our NoC model uses a traffic pattern which includes uniform random traffic and varying hot spots which send relatively large number of packets to a single receiver during a certain time interval. 10 % of the cores operate as hot spots simultaneously. The smallest data unit in the network is a packet.

The NoC model utilizes adaptive routing algorithm which favors productive routing directions but is able to overtake faulty and congested areas using non-minimal routes. U-turns are prohibited. (Dally and Towles, 2004). The algorithm determines the routing direction. The decision is based on the traffic status values and the link statuses in potential directions. A packet which cannot be delivered is put back in the router's memory and rerouted. A packet lifetime is also utilized to prevent undeliverable packets to block the network.

3.2 Monitoring Communication

The router statuses in the DCM structure are represented with two binary numbers, one for traffic status and another for fault information. In the DCM structure the status of a router is based on the occupancy of the FIFO buffer where packets are waiting to be routed forward. The occupancy of the buffer is calculated as a percentage of its size and scaled to the router status scale, which in here includes 32 different values.

In centralized and clustered monitoring structures the monitoring packets are transferred in a network similarly as the data packets. The dynamically clustered approach simplifies the monitoring communication because the routing of the monitoring packets is not needed but substituted with a packet type recog-

nition. Every monitor sends its status data and the neighbor status data it is forwarding to all its neighbors. The receiver recognizes these packets as monitoring packets and does not send them forward. A monitor stores the status data from received monitoring packets to its memory and provides this information forward to its own neighbors. This way the routers are able to receive information not only from their neighbors but also from the neighbors of their neighbors. In dynamically clustered monitoring structure the network status data spreads over the network without centralized control and without routing related processing.

3.3 Status Update Interval

A status update interval defines how often or in which circumstances a monitor sends the updated status data to its neighbors. There are two different approaches: *static* and *dynamic*. When a static update interval is used every monitor sends the updated status data to its neighbors after a certain time interval regardless of the changes in the data after the previous update. The only parameter in the static update is the time between the updates. The time interval parameter should be adjusted in a way that the network components have up to date status information but the update traffic does not strain the communication resources too much.

A dynamic update interval is based on the variation of the status values. The monitor sends the up to date status values to the neighbors when the difference between current and previous values is more than a pre-defined update threshold. This threshold is the essential parameter of the dynamic update which is adjusted correspondingly as the time interval parameter in the static update procedure. Static and dynamic status update intervals have certain weaknesses. When the network status is changing rapidly, the static status update misses a fraction of the changes. However, after a predefined time interval the status data will be exactly up-to-date for a moment. The weaknesses of the dynamic status update interval are opposite to that of the static update interval. When the network status is changing slowly, the status values can be slightly out of date for a relatively long time before the status value variation reaches the update threshold and will be updated.

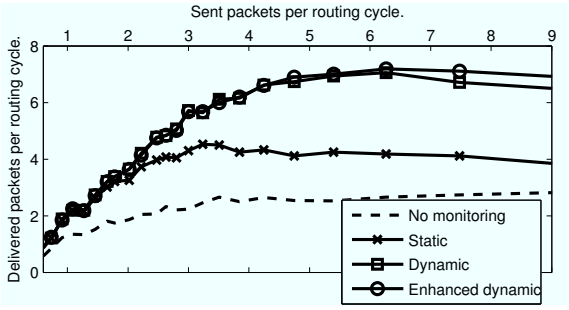

Figure 1: Throughput with different status update interval procedures and identical traffic pattern.

The weaknesses can be compensated by combining these two procedures to an *enhanced dynamic* status update interval. This interval type has two parameters which are familiar from the static and dynamic intervals: time interval and threshold. This method works similarly as the dynamic status update interval but there is also a time interval parameter which defines the maximum time between two status updates regardless of the variation of these values. When the enhanced dynamic status update interval is used, larger threshold and time interval parameters can be applied than in static or dynamic update interval. This can be used to decrease the number of monitoring packets while performance is improved.

3.4 Analysis

The influence of the different status update intervals to the network throughput were compared. Figure 1 presents throughput of a 100-router NoC with static, dynamic and enhanced dynamic status update interval protocols when 20% of links in the network are faulty. The throughput of a corresponding NoC without monitoring and adaptivity is also presented. The update interval parameters are adjusted so that the numbers of sent monitoring packets during the simulations are at a same range. In the static update interval the used time interval parameter was 17 cycles and in the dynamic update interval the threshold of four was used (status values are in range of 0–31). In the enhanced dynamic status update interval the time interval parameter was adjusted to 40 cycles and the threshold to five.

The obtained performance values with different status update intervals were compared in the range where the throughput has been saturated (an average of 7 packets sent per routing cycle). As can be seen in Figure 1 the dynamic and enhanced dynamic update intervals improve network performance significantly while the improvement with static status update interval is moderate. In a faulty network the throughput increase of 162% has been reached using the enhanced dynamic status update interval. With the dynamic update interval the obtained increase is 150%. The corresponding performance improvement with static update interval is 54%. These proposed methods make it possible to gain major improvements in the over-

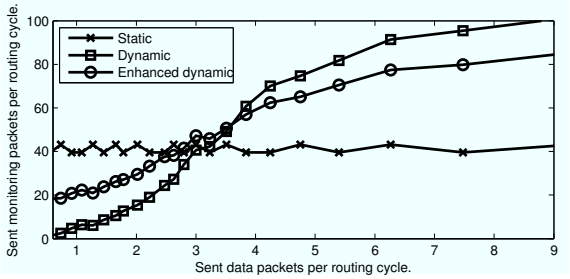

Figure 2: Number of sent monitoring packets.

all performance especially when parts of the network resources are faulty or unusable.

The number of sent monitoring packets is illustrated in Figure 2. The variation in the number of packets with static update interval is due to folding between static status update interval and the sample rate in the NoC model. As can be noted the number of packets increases with the amount of traffic when dynamic or enhanced dynamic update intervals are used. The integration of status data to the data packets will be considered in future works.

The number of monitoring packets is high related to the number of data packets. However, each monitoring packet has the hop count of 1 and they do not require routing decisions but only a simple routing packet recognition when they are moved in the network. Thus, the existence of monitoring packets is negligible compared with the obtained performance improvement. One should also note that the number of monitoring packets in highly loaded network with the enhanced dynamic status update interval is smaller than with the dynamic status update interval although the throughput is increased.

The complexity of the different status update interval implementations were analyzed using VHDL models. The status update interval control units were modeled with static, dynamic and enhanced dynamic mechanisms. These VHDL models were synthesized to 90 nm technology and the results are presented in Table 1. The modeled part is just a small piece of a monitor and a very small part of the whole system which means that the presented size differences may not be prominent. However, in some implementations the designer could choose dynamic status update interval to do a compromise between complexity and performance.

Table 1: Status update implementation complexity.

	Static	Dynamic	Enhanced dyn.
Cells	99	461 (+366%)	581 (+487%)
Area	1362 μm^2	3780 μm^2 (+178%)	5081 μm^2 (+273%)

4 CONCLUSIONS

The features of the dynamically clustered monitoring were discussed and the status update intervals were analyzed. The analysis shows that the best performance is obtained using the proposed enhanced dynamic status update interval. The proposed enhanced status data update interval decreases the amount of required monitoring traffic in a highly loaded network when compared with the dynamic status update interval. The enhanced status update interval increases system complexity but in large and complex NoCs the complexity increase is negligible.

Future work includes further development of the dynamically clustered Network-on-Chip monitoring including issues concerning status data diffusion, form of the data as well as routing and monitoring algorithms. The ultimate goal is to bundle up an intelligent, reliable and high-performance communication platform for future integrated circuits.

ACKNOWLEDGEMENTS

The authors would like to thank the Academy of Finland, the Nokia Foundation and the Finnish Foundation for Technology Promotion for financial support.

REFERENCES

Al Faruque, M., Ebi, T., and Henkel, J. (2008). ROAdNoC: Runtime observability for an adaptive Network on Chip architecture. In *IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2008*, pages 543–548.

Ciordas, C., Goossens, K., Basten, T., Radulescu, A., and Boon, A. (2006). Transaction monitoring in Networks on Chip: The on-chip run-time perspective. In *International Symposium on Industrial Embedded Systems, IES '06*, pages 1–10.

Dally, W. and Towles, B. (2001). Route packets, not wires: On-chip interconnection networks. In *Design Automation Conference*, pages 684–689.

Dally, W. J. and Towles, B. (2004). *Principles and Practices of Interconnection Networks*. Morgan Kaufmann.

Marescaux, T., Rångevall, A., Nollet, V., Bartic, A., and Corporaal, H. (2005). Distributed congestion control for packet switched Networks on Chip. In *International Conference ParCo 2005*, pages 761–768.

Mouhoub, R. and Hammami, O. (2006). NoC monitoring hardware support for fast NoC design space exploration and potential NoC partial dynamic reconfiguration. In *International Symposium on Industrial Embedded Systems, IES '06*, pages 1–10.

Nollet, V., Marescaux, T., and Verkest, D. (2004). Operating-system controlled Network on Chip. In *41st Design Automation Conference*, pages 256–259.

Rantala, V., Lehtonen, T., Liljeberg, P., and Plosila, J. (2011). Analysis of monitoring structures for network-on-chip – a distributed approach. *To be published in IGI International Journal of Embedded and Real-Time Communication Systems (IJERTCS)*.

van den Brand, J., Ciordas, C., Goossens, K., and Basten, T. (2007). Congestion-controlled best-effort communication for Networks-on-Chip. In *Design, Automation & Test in Europe, DATE '07*, pages 1–6.