Multi-objective Artificial Immune Algorithm for Security-constrained Multi-Application NoC Mapping

Johanna Sepúlveda, Guy Gogniat[1], Cesar Pedraza[2], Ricardo Pires, Wang Chau, Marius Strum
Microelectronics Laboratory LME, University of São Paulo
[1]Information and Communication Science and Technology Laboratory Lab-STICC, Université Bretagne Sud
[2]Telecommunications Engineering Faculty, Santo Tomás University, Colombia
jsepulveda, jcwang, strum, rpires@lme.usp.br, guy.gogniat@univ-ubs.fr, cesarpedraza@usantotomas.edu.co

ABSTRACT
Network-on-chip (NoC) is becoming important as the communication structure of the MPSoC (Multi-processor-System-on-Chip). Designing an optimal NoC for satisfying the MPSoC communication and security requirements involves the specification of a large set of configuration parameters. IP mapping is one of the most critical parameters in Network-on-chip (NoC) design, strongly influencing the MPSoC performance. IP mapping has been solved using single and multi-objective optimization algorithms. In this paper we propose the use of a multi-objective adaptive immune algorithm (MAIAS), *an evolutionary approach* to solve the multi-application NoC mapping problem targeting security issues, while achieving the best performance. Our results are compared with those of the genetic and branch-and-bound multi-objective mapping algorithms. MAIAS obtained better results than PBBB and MGAP in a shorter time. The experimental results showed that the MAIAS achieves configurations that fulfill the security requirements while decreasing the power consumption in 26% and the latency in 41% compared to the branch-and-bound approach and 35% and 37% over the genetic approach.

Categories and Subject Descriptors
J [**Computer applications**]

General Terms
Algorithms, Performance, Design, Security.

Keywords
Network-on-Chip

1. INTRODUCTION
MPSoC designers have to face up tight development times as well as the rapid evolution of current applications [1]. To be cost effective, SoCs are often programmable and integrate several different applications on the same chip (i.e cell-phone, personal digital assistant) [1]. Such type of system is called multi-application [2]. Current pervasive computing and flexibility in SoC design trends promote resource sharing and upgrading capabilities that integrates the SoC onto an aggressive world. SoCs can be subject of several kinds of attacks. Although sharing many of the hardware components on the MPSoC, different applications executed on the same die may present very different performance requirements and different sets of security rules, called security policy. To be security effective, SoC's IPs must be grouped together according the securities characteristics. Sensible IPs closeness advantages the implementation of hardware and software protection mechanisms. Network-on-Chip (NoC) are used as the MPSoC communication structure [4-7]. A NoC is an integrated network that uses routers to allow the communication among the IPs. Final NoC configuration must support the requirements of all the applications of the MPSoC. This paper addresses the *mapping problem*. It deals with the allocation of HW IP cores onto the network routers such that all the security and performance MPSoC requirements are met. According to [1], NoC mapping is one of the most critical parameters in NoC design. Mapping is a quadratic assignment problem that is known to be NP-hard [3]. The search space of the problem increases factorially with the system size [4]. Furthermore, the mapping solution must satisfy all the system requirements consisting of multiple desired objectives that are frequently in contrast with each other [4]. The best mapping solutions have been obtained using a multi-objective strategy [4-6]. As a result, the designer obtains a set of best mapping alternatives (*Pareto optimal set, nondominated solutions*) featuring different trade-offs among the performance indexes [4-6]. However, no one of the previous works take into account the security IP requirements. This paper is an evolution of the work presented at [6]. In this work we propose MAIAS an improved version of our Multi-objective Adaptive Immune Algorithm (M2AIA), to solve the multi-application NoC mapping problem under security constrains. MAIAS explores the mapping space producing a set of best mapping alternatives. We compared our solution with modified versions that we implemented for the PBBB (branch-and-bound) and MGAP (genetic) algorithms. The Pareto optimal set of all 3 algorithms were then evaluated and compared using a NoC-based *(SystemC-TLM)* simulation environment. The remaining text is divided into five sections. Section 2 presents an overview of the previous multi-objective mapping works. Section 3 presents the MAIAS mapping algorithm. Section 4 shows our experimental results and the comparison among PBBB and MGAP. Finally we present our conclusions in Section 5.

GECCO'12 Companion, July 7–11, 2012, Philadelphia, PA, USA.
ACM 978-1-4503-1178-6/12/07.

2. PREVIOUS WORKS
NoC mapping has been widely explored [1,4-8]. According to the number of the optimization objectives and the number of application supported by the SoC, previous works can be divided into 3 categories: 1- *Single objective and single application* [7-8]; 2- *Multiple objective and single application* [4-6]; and 3- *Single objective and multiple applications* [1]. All works [1, 4-8] used an application characterization graph (APCG) that describes the communication requirements. In [4], PBBB mapping alternatives are evaluated through event-driven trace-based simulation (dynamical model). In [5], MGAP mapping alternatives are evaluated through an analytical model (static model).

3. GENERAL DESCRIPTION

Table 1 shows the metaphors employed by MAIAS. MAIAS performs the mapping search using NoC analytical model (static evaluation). *Pareto optimal set* is then simulated through a SystemC-TLM NoC evaluation framework (dynamic evaluation) under different traffic conditions. MAIAS adopts the combination of the MPSoC APCGs, that includes security characteristics of each MPSoC application, in order to generate a synthetic APCG (Worst-Case-Security APCG), used as an entry of the optimization process. MAIAS is composed of six phases.

Phase 1: Generating the initial set of mapping alternatives (Fig 1).

Phase 2: Evaluation of the *objective functions,* power consumption and latency of all the mapping alternatives. Mappings that group IPs with similar security characteristics are rewarded.

Phase 3: Ranking of mapping alternatives according to the *dominance value* of the objective functions results

Phase 4: Refining the *Pareto optimal set*. The copied mapping alternatives are modified using two mutation operators: *shift* (random shift of IPs) and *somatic point* (random swap of two IP).

Phase 5: Ranking the remaining dominated mapping alternatives according to three parameters: 1) the objective function, 2) avidity and 3) security proximity. The purpose is to identify and penalize mapping solutions in densely populated areas.

Phase 6: Generating *M* new mapping alternatives from the crossover of the modified Pareto optimal set (phase 4) and the mapping alternatives (step 5). MAIAS stops when no more significant improvement can be expected.

Table 1. Immune system metaphors.

Immune system feature	*MAIAS*
Antigen	Security Application characterization graph (APCG)
Antibody	Mapping alternative
Pattern recognition	Multi-objective quantification
Clonal selection	Top mapping alternatives selection
Clonal suppression	Mapping alternatives elimination
Mutation	Mapping alternatives modification
Maturation	Mapping alternatives creation
Learning and memory	Mapping solutions

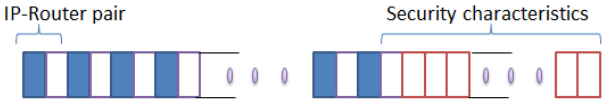

Figure 1. Mapping alternative

Table 2. MAIAS parameters

Parameter	*Value*
Initial population M (phase 2)	600
Mutation probability (phase5)	0.1
Crossover (phase6)	40%
Stop criterion	0.1

Table 3. Performance metrics

	Spacing	Spread	Execution time				
			#IP 7	#IP= 16	#IP= 25	#IP= 49	#IP= 100
PBBB	0.0223	0.9086	0%	145%	328%	564%	643%
MGAP	0.0141	0.8769	0%	67%	176%	192%	234%
MAIAS	0.0069	0.8401	0%	0.1%	0.2%	0.3%	03%

4. EXPERIMENTAL WORK

All the tests were performed on a homogeneous wormhole 2D mesh-based NoC, a XY routing algorithm, 4- flits sized buffers and a round-robin arbitration technique. Table 2 shows the MAIAS parameters. We used 8 benchmarks, each one supporting up to 6 MPSoC applications. The APCG values of each benchmark were randomly selected. MAIAS find NoC mappings that decrease the power consumption in average 26%, 35% and 62% and the latency 41%, 37% and 55% over the PBBB and MGAP and non-security constrained solution, respectively. Table 3 shows the performance comparison among the 3 algorithms according to three performance metrics: 1-Spacing *P* (distance between the mapping solutions); 2-Spread *A* (distance among all the mapping alternatives); and 3-Execution time *T* (time spent to reach stop criterion, as a percentage of a 7 IP MPSoC). The results show that MAIAS achieves a lower spacing and spread values, so that it performs a uniform exploration. Moreover, MAIAS speedups the mapping search when compared to PBBB and MGAP techniques. MAIAS also shows independence of the number of IP cores.

5. CONCLUSIONS

MAIAS is a powerful algorithm. It can be used for current MPSoCs, that integrates a high number of IPs. It was observed in simulations that taking into account security to perform the mapping reduces the power and latency consumption of the system compared solutions that only take into account the communication requirements. As future work, we plan to refine our analytical model in order to include a wider set of traffic characteristics and topologies.

6. REFERENCES

[1] Murali S., Coenen M., Radulescu A., Goosens K., De Micheli G.: Mapping and Configuration Methods for Multi-Use Case NoCs". In Proc. Asia and South Pacific DAC conference. 2006.

[2] Ascia G., Catania V.: An Evolutionary Approach to Network-on-chip Mapping Problem. In Proc. IEEE Evolutionary computation, 2005.

[3] Jena R., Sharma G.: A Multi-objective Evolutionary Algorithm Based Optimization Model for Network-on-Chip Synthesis. In Proc. Inter. Conference on Information Technology, 2007.

[4] Sepulveda M. J, Pires R, Wang C, Strum M. A multi-objective adaptive immune algorithm for multi-application NoC mapping. In Proc. Latin American CAS.conference. LASCAS 2011.