QoSS Cluster-Based NoC security implementation for multi-application SoC protection

Johanna Sepulveda, Ricardo Pires, Wang Jiang Chau, Marius Strum
Microelectronics Laboratory LME
University of São Paulo, Brazil
jsepulveda,ripires,jcwang,strum@lme.usp.br

Guy Gogniat
Information and Communication Science and Technology Laboratory, Lab-STICC
Université Bretagne Sud, France
guy.gogniat@univ-ubs.fr

Abstract—The widespread adoption of MPSoCs (Multiprocessor System-on-Chip) in critical systems, turns security into an important design requirement. MPSoCs are able to support multiple applications on the same chip. The challenge is to provide a trustworthy MPSoC and guarantee that performance and security requirements of all the applications are met. Our work implements the QoSS (Quality-of-Security-Service) at NoC (Network-on-Chip). It takes advantage of the NoC wide system visibility and critical role in enabling system operation by exploiting the NoC components to detect and prevent a wide range of attacks. In this paper, we present the implementation of cluster-based NoC architecture that integrates agile and dynamic security firewalls to protect efficiently the multi-application systems. We evaluate the effectiveness of our approach over several MPSoCs scenarios and estimate their impact on the overall performance. We show that our architecture can perform a fast detection of a wide range of attacks and a fast configuration of the different security policies for several MPSoC applications.

Keywords—Network-on-Chip; Security; MPSoC

I. INTRODUCTION

MPSoCs (Multiprocessor System-on-Chip) have been proposed as a promising architecture choice to overcome the new system requirements. MPSoCs are programmable and able to integrate different applications on the same chip (i.e. cell-phone, personal digital assistant) [1]. Such type of system is called multi-application. Each application is characterized by a set of performance and security requirements (security policies). Therefore, there is no a single and static security requirement, but a set of ever changing security policies that must be satisfied. The MPSoCs security policy must be able to supply different levels of security and be capable of changes during operation time. Due to the intrinsic embedded constraints and strict requirements, the implementation of security is considered as a challenging task. MPSoC can be attacked via hardware/software [2]. Software attacks are responsible for 80% of security incidents [3]. All software attacks start with an abnormal communication. In this paper we address protection of the MPSoC against software attacks by implementation of security policies at the NoC (Network-on-Chip). NoC has become an attractive alternative as a communication structure for MPSoCs. A NoC is an integrated network that uses routers to allow the communication among computation components. Security integration at NoC is naturally advantageous [2]. NoC may contribute to the overall security of the system, providing the ideal mean for monitoring systems behavior and detecting specific attacks [2]. The communication structure is becoming the heart of the MPSoC [3]. It has a significant impact on the overall MPSoC performance. To make feasible MPSoC protection by NoCs, the security policy must be customized in order to provide a better trade-off between system performance and security. Our work proposes the implementation of QoSS (Quality of security service) to overcome present SoC vulnerabilities. QoSS introduces security as a dimension of QoS (Quality-of-Service). In contrast with previous works, different security levels deployment allows the best tradeoff between system security and performance requirements. QoSS at Network-on-Chip (NoC) provides predictable performance while guaranteeing the desired protection level. Our cluster-based NoC architecture efficiently meet the changeable MPSoC security requirements. It distributes the security policy management by partitioning the NoC topology into different security zones (low NoC), ruled by a local security policy and connected through a global interconnect (high NoC), ruled by a global security policy. Each zone integrates a set of mechanisms capable of being configured according to QoSS needs of each application. We show that our architecture can perform a fast detection of a wide range of attacks and a fast configuration of the different security policies for several MPSoC applications. The experiments were performed using a SystemC-TLM timed simulation framework. It automatically carries out performance evaluations for a wide variety of MPSoC scenarios.

II. PREVIOUS WORKS

Security integration at the NoC level was addressed in the works of [2-3]. These works show that NoC can be a useful structure to handle different security services. However, the adoption of these previous solutions to address MPSoC security challenges present three main limitations. 1) They implement a single NoC security level for the entire SoC; 2) They implement static security policies; and 3) They are not appropriate for multithreaded systems. In our previous work [4] we developed a dynamical NoC-based protection for SoCs. However it uses central control blocks that present a strong impact on the overall area due to link overhead. The purpose of the present work is to overcome these limitations.
III. GENERAL DESCRIPTION

Our security architecture is based on a cluster-based NoC (CNoC). It is constituted by a set of low NoCs that exchange information through a high NoC. CNoC is noted as $n(S_1)/(S_2)$, where $n$ is the number of clusters, $S_1$ is the low NoC size, and $S_2$ is the high NoC size. Fig 1. shows a $4(2x2)/(2x2)$CNoC.

Fig 1. CNoC 4(2x2)/(2x2).

A. Components

The IP components are mapped on the CNoC according to their communication and security characteristics by using the MAIAS algorithm [4]. The purpose is to allocate in the same security zone the IPs with higher communication frequency and similar security requirements. Our architecture integrates five key components:

1) **Low/High NoCs**: Each cluster is connected through a low NoC, ruled by a local security policy. High NoC collects the traffic coming from different clusters, ruled by the global security policy.

2) **Policy keeper**: It stores the security policies (local and global). It integrates the information of the MPSoC thread scheduler, the clusters and the access rules (rights) of each thread being executed on the MPSoC.

3) **Configuration Control**: Coordinates and configures the security mechanisms of the MPSoC according to the local and global security policies of each application.

4) **Security mechanisms**: Protect the MPSoC against possible attacks by means of firewalls embodied in the NoC (low and high).

5) **Monitors**: Audit the high NoC and low NoC communication behaviour. It determines the completion of each communication event between different master/slave pairs of the MPSoC and abnormal communication patterns.

B. Functionality

When the MPSoC security policy must be upgraded, the configuration control starts five procedures: 1) lookup policy keeper, downloading the proper local and global security policies, stored in the policy keeper component; 2) block, interrupting the injection of packets whose final destination is the processing component linked to the security zone that is going to be reconfigured; 3) look-up monitors, determining the start of the configuration; 4) global configuration (high NoC) and local configuration (low NoC), upgrading the security tables at the firewalls; and 5) unblock, normalizing the data injection.

IV. EXPERIMENTAL WORK AND RESULTS

We develop a CNoC 4(2x2)/(2x2) SystemC-TLM cycle-accurate model. CNoC is characterized by a XY routing scheme, round-robin(RR) arbiter and FIFO memory organization. The proposed solution has been verified against three types of attack scenarios: 1) Extraction; 2) Modification; and 3) DoS. We tested 3 applications of MiBench benchmark suite [5]: auto/industrial (A1), consumer electronics (A2) and telecommunication (A3). Each application is characterized by a security policy that establishes different levels of authentication and access control security mechanisms. Table I shows the results of the efficacy of our security implementation. It represents the percentage of attacks detected by the security mechanisms. Figure 2 shows the latency and power distributions over all the components of our CNoC. They show that the security interfaces and the policy keeper are the components that consume more time and power, respectively.

![Table I. Security Efficacy](image)

V. CONCLUSIONS

Our cluster-based approach provides three advantages: 1) facilitates the security management of the MPSoC; 2) produces smaller security tables; and 3) improves system performance. Two techniques are employed in order to achieve an efficient configuration: 1- security mechanisms are implemented hierarchically therefore avoiding interruption in NoC execution; and 2- QoS (Quality-of-service) mechanisms are employed to provide predictable penalties while the network interfaces are modified.

REFERENCES


