Problems and Challenges of Emerging Technology: Networks−on−Chip

Introduction

The advancement of technology makes it possible to stack many different cores with the same or different processing elements, memory, intellectual property (IP), etc. in a multi-layer single chip. bottleneck. In fact, conventional buses cannot keep up with the bandwidth and complexity of recent multiprocessors or multiprocessor chips. Due to the heterogeneity of the latest chips and the large number of internal cores (for example, modern system-on-chips (SoC)), system designers must deal with multiple clocks and multiple power domains, long wires, and many other issues.

Another bottleneck pointed out by the industry is the mismatch abstraction between the core and the bus. When a higher level of abstraction is aimed at minimizing the details that system designers have to deal with, interconnection logic forces them to consider interconnection constraints when designing functional cores or IP. System designers are forced to work at a lower level of abstraction, so a question is raised as to whether the benefits of relying on highly integrated technologies are trustworthy. Many industry participants, for example, at that time, ARM relied on its AMBA agreement or VSI alliance's efforts to focus on matching the core with the bus.

The essence of the network-on-chip (NoC) paradigm is that when extended to this heterogeneity and/or the dimensionality of the core, the concept of on-chip interconnection has changed from a traditional bus to a complex network. Part of the potential of the NoC concept lies in the complete separation of computing and data transmission. Even in the early design stage, this will allow the use of decoupled design methods. Therefore, system designers working at the top level of the project can make progress in the design process of the required SoC without worrying about protocol and width conversion, as well as the issues of multiple clocks and multiple power domains. Heterogeneity and conversion problems can be solved only through the NoC layer. The key contribution to the bus-based basic chip design process lies in performance, power consumption, chip size and project design time. The last two contributions are the key factors that enable the NoC concept to persist and be adopted in the industry.

When switching from classical NoC to emerging technology NoC, many concepts change essentially, but not exclusively, due to the technology shift. Emerging technology NoC are investigated as a response to the higher demands of future applications in terms of bandwidth and energy efficiency. In fact, higher data band- widths up to 100 s of Gbps with optical NoC (ONoC) and up to 10s of Gbps with wireless NoC (WiNoC) can be achieved with limited transmission losses. In addition, when the link dis- tance between the communicating nodes is important, ONoC or WiNoC overcome conventional NoC. The energy dissipation per bit in function of the distance is lower for ONoC and WiNoC compared to the conventional ones. In terms of latency, emerging technology NoC can alleviate multi−hops data transmission. With 3D NoC, the additional dimension adds an extra alternative to circulate data. With ONoC, an optical channel can be shared between the chip nodes resulting on a general one−hop data transmission. With WiNoC, several islands of wired cores can be connected wirelessly resulting on a general two or three hops data transmission. From this perspective, higher levels of data throughput were obtained in practice such as in for WiNoC (up to 18Gbps) and for ONoC (up to 100Gbps).

Challenges for Emerging Technology NoC

Energy efficient NoC with high data throughput capability

The pursuit of high-efficiency NoC with high throughput is the main reason for the exploration of emerging technology NoC. From this perspective, the hybrid approach is a viable solution. For example, the combination of conventional NoC and optical NoC is very interesting. Conventional NoC can handle local and repeated transactions, while ONoC can handle remote transactions or transactions with higher throughput. The same method can be applied to WiNoC. WiNoC can be used to connect multiple islands of PE locally connected with traditional NoC. In addition, the new substrate material can provide higher yields while having a reasonable cost of power consumption.

Security

For the NoC paradigm, many aspects must be reconsidered, and the future SoC is most likely to use NoC as an interconnection infrastructure. As a first attempt, Fiorin et al. [1] discussed NoC security challenges through existing work. The first is how to use NoC to protect SoC, and the second is how to authenticate the SoC security mechanism based on secure NoC.
Work in this area is focused on using NoC to protect the system. However, newer methods assume that in the case of a NoC purchased by a third party, the NoC itself may be the source of the threat.

Problems and Challenges of Emerging Technology: Cyberattack

Introduction

Safe operation in cyberspace is a global information flow network associated with the Internet, which is vital to the continued operation of the international economy and many other areas. The Internet is an extraordinary tool for many purposes. It is also vulnerable to attacks by hostile intruders, whether it is to spread misinformation, damage important infrastructure or steal valuable data. Most of these malicious activities are carried out by individuals or groups of people who try to enrich themselves or influence public opinion. However, it is becoming more and more obvious that government agencies that often cooperate with some of them are using cyber weapons to weaken the enemy by sowing mistrust or undermining key institutions, or to enhance their defense capabilities by stealing military-related technical knowledge.

In addition, if there is a crisis or hostilities, cyber attacks may be launched on the adversary's early warning, communication and command and control systems, which will severely weaken its response capabilities. For all these reasons, network security or the protection of cyberspace from malicious attacks has become the top priority of national security.

Chalenges for Cyberattack

In many respects, the cyber domain has become similar to the strategic nuclear domain. The concepts of defense, deterrence, and guaranteed retaliation that were originally designed for nuclear scenarios have now been applied to cyberspace conflicts. Although fighting in this area is said to have fallen below the threshold of armed combat, it is not difficult to imagine violent skirmishes erupting in cyberspace, for example, if a cyber attack causes the collapse of critical infrastructure.

Cyberspace is only regarded as an area of its own. Although the introduction of cyber weapons instead of nuclear or conventional ammunition is fertile ground for the implementation of regulatory measures, it can be said that these measures are similar to arms control. This is not a new challenge, but a challenge that has become more and more urgent with the development of technology. For example, when will such a digital attack paralyze the critical information systems of other countries?

References

1. Fiorin, Leandro, Cristina Silvano, and Mariagiovanna Sami. "Security aspects in networks-on-chips: Overview and proposals for secure implementations." In 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2007), pp. 539-542. IEEE, 2007.