Secure Network-on-Chip Architectures for MPSoC: Overview and Challenges

Luka Daoud
PhD Candidate in Electrical and Computer Engineering
Boise State University, Boise, ID 83725
Email: LukaDaoud@u.boisestate.edu

***Abstract*—Network-on-Chip (NOC) is the heart of data communication between processing cores in Multiprocessor-based Systems on Chip (MPSoC). Packets transferred via the NoC are exposed to snooping, which makes NoC-based systems vulnerable to security attacks. Additionally, Hardware Trojans (HTs) can be deployed in some of the NoC nodes to apply security threats of extracting sensitive information or degrading the system performance. In this paper, an overview of some security attacks in NoC-based systems and the countermeasure techniques giving prominence on malicious nodes are discussed. Work in progress for secure routing algorithms is also presented.**

Keywords*—Network-on-Chip, NoC, Hardware Trojan, HT, Secure Routing Algorithm, Malicious-Tolerant Routing Algorithms.

I. Introduction

The Advances in technology have unprecedented growth in the semiconductor industry, so the complexity of circuits built on a single chip has been increased. In order to keep pace with such sophisticated levels of integration, design engineers have come up with a new design methodology, known as System-on-Chip (SoC). For clock frequency scaling and high throughput systems, Multiprocessors System-on-Chip (MPSoC) [1] are now the only way to construct a high performance platform by filling up a processor die with multiple simpler processing elements (PEs). Future designs are expected to integrate hundreds of PEs into a single chip. Therefore, an interconnect architecture, that provides a communication mechanism, must exist among the PEs. For large number of PEs in a MPSoC, traditional bus-connection has poor flexibility and performance. Hence, Network-on-Chip (NoC) Architecture [2] has been proposed as a high performance, scalable and power efficient alternative.

Although the advantages provided by NoC for integrating complex systems, modern SoC are exposed to a plethora of security attacks. In MPSoC, the processing cores are allocated with multiple different applications that are running simultaneously [3]–[5]. Data are exchanged among the applications through the NoC in plaintext. As a result, data are vulnerable to security threats such as: a malicious application may be mapped to some PEs and steal sensitive information of other applications exploiting the on-chip network. Moreover, a malicious application can be run on the MPSoC applying a denial of service (DoS) attack by injecting redundant packets to throttle the NoC and consequently it degrades the overall system performance.

As far as security attacks in SoC is concerned, the malicious hardware modification of the original design in the chip, known as Hardware Trojan (HT) [6] plays a vital role in security threats, where the hardware platform becomes insecure. The aim of such HT attacks are to leak information, degrade the system, manipulate data, or others [7], [8]. HTs can be embedded during any stage of the IC design flow and/or during manufacturing process. They are becoming more complex and powerful such that they are hard to detect, particularly in complex systems on a single IC, which makes the test processes even harder to notice HTs. Since NoC is composed of several different based-routing modules, network interfaces, and various control units, the complexity of NoC has increased and made it vulnerable to HT attacks.

Our proposed research investigates the impact of Hardware Trojans in NoC and presents a secure Network-on-Chip architecture, focusing on secure and malicious-tolerant routing algorithms with HT runtime detection. The rest of this paper is organized as follows; security attacks in NoC-based systems are explored in Section II, malicious NoC and research challenges are discussed in Section III. Conclusions and future work are described in Section V.

II. Security Attacks in NoC-based Systems

Most of NoCs have been developed without compromising security issues in the design. So far, most of the proposed solutions try to secure the cores and not the intercommunication media inside the MPSoC. Table 1 summarizes several goals of security attacks in NoC and the proposed countermeasures. In system degradation, the goal of such attack is to degrade the whole system through applying Denial of Service (DoS) by wasting the network bandwidth through flooding the NoC with redundant packets, deadlock, or livelock. On the other hand, power deprivation attack aims to waste more power in the NoC by any means such as deviating the packets in the network to consume more power to reach their destinations. In secret information extraction, sensitive information are attacked by an unauthorized read or side-channel attacks. However, Hijacking (System Reconfiguration) attack is the most harmful threat since all security policies are ineffective if the system can be configured/reconfigured by an attacker. In this case, users fail to have control on the system.

In order to react to such attacks, firewalls are build in the network interface of the NoC to filter malevolent and unauthorized packets. In security zones technique [9], PEs

978-1-5386-7392-8/18/$31.00 ©2018 IEEE

that are mapped to run a sensitive application follow a certain security-policy. Another technique to protect the secrecy of the data in the NoC is by applying encryption protocols [10]. Secure routing algorithm is one of the important techniques to avoid malicious nodes that participates in the security threats. The main challenge of such secure routing schemes is detecting the malicious nodes, which is a part of our work in progress. Once the malicious routers have been detected, the secure routing protocol detour packets around them. In our research work [11], a HT is embodied in the NoC to violate the routing protocol causing deadlock to apply DoS attack. [11] proposed a routing aware scheme to detect the HT in runtime and detour the packets around such malicious nodes.

TABLE I. ATTACKS SCENARIOS IN NOC AND COUNTERMEASURE TECHNIQUES

Attack Goal	**Attack Method**	**Countermeasure Technique**
System Degradation	Denial of Service: Bandwidth depletion Incorrect path Deadlock Livelock Power Deprivation	Firewall Security Zone Encryption Secure Routing
Secret Information Extraction	Unauthorized Read Side-Channel	
Hijacking	Unauthorized Write Unauthorized Reconfiguration	

III. MALICIOUS NOC AND RESEARCH CHALLENGES

Most of the aforementioned security attacks are software-based, where they can be revoked by firmware and software updates. However, what if the hardware platform itself is malicious? In this section, we explore the research challenges in infected NoC with malicious routers. Attackers can embed HTs in the routing nodes to apply security threats, such as extracting sensitive information or system degradation. A Trojan in hardware can be in an idle state and waiting for an activation (trigger) signal to run its malicious payload. This made the HT potent and very difficult to reveal during post-silicon tests. Malicious nodes can be classified as follows:

- **Benign node** - a malicious node that can be detected and automatically avoided by the system routing technique. For example, a faulty node that does not respond to routing can be avoided by an adaptive routing technique, but for multiple faulty nodes or deterministic routing, they are absolutely harmful nodes.
- **Moderate-harmful node** - a malicious node that is hard to detect and expensive to be avoided. For instance, infected nodes that apply DoS by flooding the network with redundant packets. It is hard to detect and needs more effort to distinguish between DoS attack and normal traffic.
- **Malignant node** - a malicious node that is very hard, mostly impossible, to detect and silently applies its payload. For example, a node that corrupts packets without detection, known as silent data corruption, or a black hole router that follows the communication handshaking but drops the packets without forwarding them to the next hop is a highly harmful for the NoC and risky for the running applications.

The main goal of this research is to detect such malicious nodes at run-time and avoid them through secure routing techniques. Unlike fault-tolerant routing algorithms where the faulty nodes are dead routers and are not involved in packets' routing, malicious nodes are nodes that participate in packets routing and apply their payload to breach the system security or degrade the system. In contrast to malicious nodes, faulty nodes are easy to be detected and avoided. On the one hand, malicious nodes are seemingly part of the network, but on the other hand they attack the system as soon as they are triggered. Run-time detection and avoiding such malicious nodes are the current research challenges.

IV. FINAL REMARKS

Multiprocessors System-on-Chip (MPSoC) are now the only way to construct a high performance platform, where multiple processing cores are connected and communicating through Network-on-chip (NoC). NoC is flexible and dynamically allow application sharing resources in MPSoC, which makes the NoC security critical. NoC may be infected with Hardware Trojans (HTs) aiming to steal information, control, or degrade the system. The challenge is to provide a secure on-chip network that allows a trustworthy network platform for applications running in the system. The current research focuses on the impact of Hardware Trojans in the NoC and provide a secure routing algorithm.

REFERENCES

[1] K. Olukotun, L. Hammond, and J. Laudon, "Chip multiprocessor architecture: techniques to improve throughput and latency," *Synthesis Lectures on Computer Architecture*, vol. 2, no. 1, pp. 1–145, 2007.

[2] L. Benini and G. De Micheli, "Networks on chips: A new soc paradigm," *computer*, vol. 35, no. 1, pp. 70–78, 2002.

[3] L. B. Daoud, M. E.-S. Ragab, and V. Goulart, "Faster processor allocation algorithms for mesh-connected cmps," in *Digital System Design (DSD), 2011 14th Euromicro Conference on*, pp. 805–808, IEEE, 2011.

[4] L. B. Daoud, M. E.-S. Ragab, and V. Goulart, "Processor allocation algorithm based on frame combing with memorization for 2d mesh cmps," in *Circuits and Systems (LASCAS), 2012 IEEE Third Latin American Symposium on*, pp. 1–4, IEEE, 2012.

[5] L. Daoud and V. Goulart, "High performance bitwise or based submesh allocation for 2d mesh-connected cmps," in *Digital System Design (DSD), 2013 Euromicro Conference on*, pp. 73–77, IEEE, 2013.

[6] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, 2010.

[7] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware trojan design and implementation," in *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on*, pp. 50–57, IEEE, 2009.

[8] J.-P. Diguet, S. Evain, R. Vaslin, G. Gogniat, and E. Juin, "Noc-centric security of reconfigurable soc," in *Networks-on-Chip, 2007. NOCS 2007. First International Symposium on*, pp. 223–232, IEEE, 2007.

[9] J. Sepulveda, D. Flórez, V. Immler, G. Gogniat, and G. Sigl, "Efficient security zones implementation through hierarchical group key management at noc-based mpsocs," *Microprocessors and Microsystems*, vol. 50, pp. 164–174, 2017.

[10] D. M. Ancajas, K. Chakraborty, and S. Roy, "Fort-nocs: Mitigating the threat of a compromised noc," in *Proceedings of the 51st Annual Design Automation Conference*, pp. 1–6, ACM, 2014.

[11] L. Daoud and N. Rafla, "Routing aware and runtime detection for infected network-on-chip routers," in *IEEE 61th International Midwest Symposium on Circuits and Systems (MWSCAS)*, IEEE, 2018.