A Study of Wired, Wireless, and Network-on-Chips Security

Alka Verma, Associate Professor,
Department of Electrical and Communication Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- alkasinghmail@rediffmail.com

ABSTRACT: In the design of multiprocessor system-on-chips, network-on-chips (NoCs) have been extensively utilized as a scalable communication solution (MPSoCs). NoCs enables processor cores to gain better performance by outsourcing communication activities to on-chip Intellectual Property (IP) cores. The NoC paradigm is built on the concept of resource sharing, in which hardware resources like as buffers, communication connections, routers, and so on are shared across all MPSoC IPs. In reality, the data that each NoC router routes may or may not be linked to the router's local core. Unauthorized accesses/modifications of intermediary routers, for example, may jeopardize the integrity and confidentiality of data being routed in a NoC. Many papers in the literature have identified and addressed security flaws in NoCs, with the goal of improving the NoC paradigm's security. To our knowledge, however, there is no comprehensive survey research on the security risks and countermeasures for NoCs. The security risks and solutions suggested thus far for wired NoCs, wireless NoCs, and 3D NoCs will be reviewed in this article. The purpose of this article is to provide readers with an understanding of the assaults as well as the flaws and strengths of responses.

KEYWORDS: Network-On-Chip, Threat Model, Hardware Security, Hardware Trojan, DOS Attack.

1. INTRODUCTION

Multi-Processor System-on-Chips (MPSoCs) can now accommodate tens of Intellectual Properties (IPs), such as processor cores, memory modules, and different I/O components, thanks to ever-shrinking VLSI technology. As a result of this technological transition, an effective communication architecture is required to allow rapid, but energy-efficient data transfer across the chip. Network-on-Chips (NoCs) were originally proposed in 2004 as a scalable communication architecture, and have since been extensively utilized in the design and manufacture of numerous chips. Because most contemporary MPSoCs utilize an on-chip network as their backbone communication architecture, the industry has already begun to provide NoC IPs to make the design process easier [1].

The primary concept of on-chip networks is to share resources in order to maximize resource usage, which is accomplished by connecting a number of on-chip components through a shared network controlled by a set of structural, routing, switching, and flow-control rules. The hierarchical design of NoCs helps to minimize lengthy communication cables (also known as long interconnects), which are significant contributors to dynamic power consumption and reliability problems. With moderate performance/energy efficiency, NoCs provide excellent resource utilization, design flexibility, and support for parallel communications. The low efficiency of NoCs stems from I communications between distant cores, where messages must be passed through a lengthy chain of neighboring routers, and ii) one-to-many message broadcast scenarios, which must be handled sequentially. Researchers have proposed the addition of wireless communications through wireless routers to solve these flaws. Far-distant communications and one-to-many messages are transmitted in a one-hop manner via wire-less links/transceivers in a WNoC (Wireless Network-on-Chip), improving overall performance and energy efficiency [2].

While performance elements of NoC have been addressed in many proposals/papers over the years, security has remained a significant issue for designers. When data integrity and confidentiality are critical, the concept of an on-chip network that readily accesses/forwards messages from various IP cores chip-wide may exacerbate security problems, i.e., the advantage obtained by resource sharing in NoC fabrics may be counter-productive [3].

SoC designers often use 3rd-party IPs (3PIPs) to circumvent the expensive cost and design time of MPSoCs. Processing cores and DSP units could be among the IPs, as could the NoC itself [4]. As part of the MPSoC, NoC IPs are extensively utilized in various devices such as tablets, mobile phones, and autonomous cars. The Arteris FlexNoC connection is used by 80 percent of the top five Chinese fabless firms . Because of the shorter time-to-market and cheaper manufacturing costs, MPSoC designers prefer to utilize the 3PIP (third-party IP) NoC. However, including 3PIPs products in the design of MPSoCs may result in additional security risks, like as security flaws or threats. Some of the 3PIPs may have been infected with a Hardware Trojan (HT) . This includes IPs created in-house with the help of a trusted design team and CAD tools like Synopsys and Cadence [4]. A foundry might infect them at the post-design stage . Because HT-infected IPs utilize particular trigger circumstances that make them more difficult to detect , they mostly avoid verification and production testing processes. When activated, HTs may have a significant impact on the chip's functioning. A successful assault may result in irreversible economic and societal damages that are difficult to pay for.

A hostile action often targets at least one of the main security criteria, such as confidentiality, integrity, and availability, which are referred to as the CIA trinity and are described as follows:

- Confidentiality: Only authorized agents should have access to sensitive information.

- Communication integrity: Unauthorized agents are not permitted to change the contents of a message.

- Availability: During operation, network resources stay available.

Attackers attempt to compromise these three security elements, thus SoC designers must achieve and maintain security objectives in order to protect the system. While NoC security has been briefly discussed in several earlier publications, we are unaware of any comprehensive study that examines current security solutions for different NoC technologies. For wired, wireless, and 3D NoCs, this article addresses both the various attack models and the suggested defenses [4].

Packets in wireless NoCs (WiNoCs) may go via one of two paths: the traditional wired NIs, routers, and channels, or the shared wireless medium via the NI's wire-less interfaces and wireless signal transceivers. The wireless hub is essentially a NoC router with a wireless interface linked to an additional port. Some studies assume that all routers are linked to wireless interfaces, while others assume that the network is split into clusters, with each cluster connected to a single wireless hub to save design costs. Applications such as cache coherency protocols are executed very quickly with WiNoCs because to the millimeter-wave omnidirectional antennas that are often used in WiNoCs. WiNoCs, for example, may transmit a 64B cache line anywhere in 5–15 cycles [5].

2. DISCUSSION

Taxonomy and Attacks

Physical assaults require physical access to the chip in order to carry out the malicious action, such as reading internal/external signals, accessing NoC channels, or monitoring the device's power profile. Physical assaults may take the following forms:

1) intrusive, in which the attacker dissects the packaging of the victim chip for more thorough analysis, such as probing attacks; nevertheless, the chip must remain functioning after decapsulation, or

2) Non-invasive, in which the chip is not physically modified. Non-invasive physical assaults, such as power side-channel attacks, are less expensive and simpler to implement.

Physical assaults are limited in their application due to the need for physical access. Non-physical assaults, on the other hand, do not need physical access to the chip, making them easier to use in MPSoCs. The remainder of this section evaluates and categorizes non-physical security threats [6].

Malware Injections and Hardware Trojans, which introduce malicious IP, malicious NoC, or a mix of both, are the two main sources of non-physical assaults in MPSoCs. Malware-infected IP addresses account for 80% of all assaults on embedded systems. Malware infections are most common during the device firmware/software update/patching process, when software interacts with bare-metal hardware.

After being activated, HTs are small circuits that begin their destructive activities. The triggering portion of HTs looks for very uncommon circumstances (mostly a set of signals acquiring their rare values). As a result, the majority of conventional logic testing techniques fail to identify HTs. Because HTs have small power and area footprints, side-channel analysis techniques might be useful [7].

HT-induced failures in NoC-based MPSoCs have been studied by a number of researchers. Different agents may introduce HTs at different phases of the design production process. a few scenarios for insertion are as follows:

- An opponent designer may introduce HTs by manipulating the NoC netlist at the gate level.
- EDA tools may also introduce HTs into a company's goods for defamatory reasons.
- The arrangement of the designs may be changed throughout the manufacturing stage.
- 3PIPs used to speed up MPSoC design may be contaminated with HTs beforehand.

Various HT circuits for processing/NoC IPs have been suggested by researchers. We only look at NoC HTs in the remainder of this section since HTs suggested for processing IPs are outside the scope of this study.

A malicious NoC [8] is one in which the NoC fabric contains at least one malicious Network Interface (NI) or a malicious router. To infect the NoC, either the NoC vendor or the manufacturing facility may introduce HT circuitry into the clean NoC design. HT insertions aim for I the network interface to change data packetizing/de-packetizing or flow control, or ii) the router logic to negatively impact route computation, resulting in packet misroute/loss/duplication, or to inject low-priority packets to learn about the timing information of high-priority packets.

Confidentiality, as one of the most important aspects of security, refers to the protection of a system's assets against unauthorized access. This is similar to ensuring that messages/packets transiting the network are kept private between the sender and recipient nodes in the NoC environment. Packet encryption is one of the methods for ensuring data secrecy in NoCs for this purpose. Based on our research, we believe that attacks that compromise data confidentiality are a serious threat. The following is a summary of the NoC context:

• Eavesdropping: an unidentified opponent, such as a malicious router or a router with an IP address, sniffs data transmission between a source and a destination node. Sensitive information, such as passwords or encryption keys, may be included in the data [7].

• Differential Cryptanalysis: similar to differential power analysis assaults, the attacker attempts to estimate the encryption key by studying the transmitted data across a channel. In most instances, a rogue router and a malicious IP are required to carry out the assault [9].

• Timing Attack: Intentional collisions between the attacker's data and other people's sensitive data on a particular route are used to provide the attacker important information about the sensitive data's timing and volume. The essential concept is that the attacker calculates the timing delay of their own data as a function of whether or not sensitive data is present on the same route.

• Spoofing: obtaining unwanted access to data by impersonating someone else. The accessed data may be a section of shared memory that isn't accessible by default.

• Man-in-the-middle (MITM): an unauthorized node interferes with communication between two source and destination nodes in order to monitor the data transmitted.

2.1. MAINTAINING DATA ACCURACY AND INTEGRITY

A message receiver may check whether or not the received message has been tampered with since the NoC fabric can achieve data integrity. In certain studies, researchers have jointly addressed the integrity and authenticity, like in many instances when data integrity may be accomplished via sender authentication. In NoC-based MPSoCs, there are three main methods to ensuring data integrity and authenticity.

I. Data integrity is only addressed by using error detection/correction codes and/or unkeyed hash algorithms.

II. To handle both data integrity and authenticity, keyed hash functions and message authentication codes are combined. iii) For authentication-only reasons, including physically unclonable capabilities. After a brief examination of the preliminaries of the stated methods, we examine articles addressing data integrity/authenticity in this part.

A cryptographic hash function is a one-way mathematical function that, regardless of the size of the input message, generates a fixed-length message digest. A message digest is the result of the hash function. The one-way attribute ensures that the message digest cannot be used to extract the input data. After computing the hash of the input data, it is added to the original message and delivered to the recipient. The receiver verifies data integrity by applying the hash algorithm on the body of the message and comparing the result to the received tag. Because the message space may be much larger than the hash digest space, the hash functions employed must be collision-resistant, which means that no two messages with the same hash digest can be discovered [10].

2.2. ACCESS PERMISSION

Before allowing data access, the identity of the requesting router/IP must often be confirmed. As a result, a set of rules known as access control may be used to restrict access to certain IP addresses. During the authorization process, a malicious requesting IP/router known as an Initiator targets valuable data assets in order to accomplish the following objectives [90]:

• Reading from limited memory locations to get hidden information.

• Reducing system bandwidth by flooding the network with excessive memory requests. • Changing system configuration by writing into restricted addresses. (See Subsection IV-D for further information on this case.)

3. CONCLUSION

We evaluated most of the articles released since 2015 on the security of NoC-based MPSoCs in this review study. The paper's primary aim is to provide insight to researchers in the area so that they may more easily evaluate and compare the state of the art in safe MPSoCs. This review article also identifies topics that have still to be addressed. The remainder of this part examines the unresolved issues in the design of secure MPSoCs, as well as our recommendations on how to overcome them. This section, we think, will be helpful in guiding future research in the design of safe MPSoCs.

REFERENCES:

[1] P. Hamalainen, M. Hannikainen, T. Hamalainen, and J. Saarinen, "Hardware implementation of the improved WEP and RC4 encryption algorithms for wireless terminals," 2000.

[2] V. B. Kirubanand and S. Palaniammal, "Study of performance analysis in wired and wireless network," *Am. J. Appl. Sci.*, 2011, doi: 10.3844/ajassp.2011.826.832.

[3] Jyoti and H. Saini, "A Study on Networks and Comparison of Wired , Wireless and Optical Networks," *Int. J. Innov. Res. Comput. Commun. Eng.*, 2017.

[4] M. Abdur, S. Habib, M. Ali, and S. Ullah, "Security Issues in the Internet of Things (IoT): A Comprehensive Study," *Int. J. Adv. Comput. Sci. Appl.*, 2017, doi: 10.14569/ijacsa.2017.080650.

[5] S. A. Jafar, "Topological interference management through index coding," *IEEE Trans. Inf. Theory*, 2014, doi: 10.1109/TIT.2013.2285151.

[6] B. Sikdar, "A study of the environmental impact of wired and wireless local area network access," *IEEE Trans. Consum. Electron.*, 2013, doi: 10.1109/TCE.2013.6490245.

[7] H. J. Lee, N. Park, and Y. Hwang, "A new dimension of the digital divide: Exploring the relationship between broadband connection, smartphone use and communication competence," *Telemat. Informatics*, 2015, doi: 10.1016/j.tele.2014.02.001.

[8] J. Sepúlveda, A. Zankl, D. Flórez, and G. Sigl, "Towards Protected MPSoC Communication for Information Protection against a Malicious NoC," 2017. doi: 10.1016/j.procs.2017.05.139.

[9] E. Alotaibi and B. Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks," *Computer Networks*. 2012. doi: 10.1016/j.comnet.2011.10.011.

[10] D. Du, B. Qi, M. Fei, and Z. Wang, "Quantized control of distributed event-triggered networked control systems with hybrid wired–wireless networks communication constraints," *Inf. Sci. (Ny).*, 2017, doi: 10.1016/j.ins.2016.03.033.