INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	MANJU R
Roll Number	:	186101012
Programme of Study	:	Ph.D.

Thesis Title: Hardware Trojan Mitigation for Securing Network-on-Chip Communication Against Packet Routing Attacks

Name of Thesis Supervisor(s)	:	Dr John Jose
Thesis Submitted to the Department/ Center	:	CSE
Date of completion of Thesis Viva-Voce Exam	:	13.09.2024
Key words for description of Thesis Work	:	Network-on-Chip, Hardware Trojan, DoS attacks

---

SHORT ABSTRACT

As Tiled-Chip Multi-core Processors (TCMPs) become widely adopted in automotive systems, IoT devices, and consumer electronics, securing them against hardware attacks is critical. Among these, Hardware Trojans (HTs) pose a major risk to TCMP reliability, especially in Network-on-Chip (NoC) interconnects, which are vulnerable to attacks like information leakage and bandwidth denial. This thesis examines HT attacks on NoC architecture and proposes novel detection and mitigation strategies to safeguard TCMPs. The work addresses three key HT-induced Denial of Service (DoS) attacks: Packet misrouting, Packet looping, and Packet duplication. For each, techniques are proposed to detect, localize, and neutralize threats within the NoC. The thesis begins with a survey of HT attacks in TCMPs, highlighting their impact on performance and security. The first major contribution focuses on mitigating packet misrouting DoS attacks through a dynamic shielding technique and secure routing algorithm to isolate compromised NoC routers. The second contribution addresses HT-induced packet looping attacks, proposing a security wrapper and path monitoring to limit delays with minimal performance impact. Finally, the third contribution tackles HT-induced packet duplication, introducing a Packet Status Holding Register to prevent duplication with low hardware overhead. Experimental results show significant improvements in packet latency and throughput.