Chapter 11
Reliability and Security Challenges in Electrical/Optical On-Chip Interconnects for IoT Applications

Muhammad Rehan Yahya
https://orcid.org/0000-0002-6777-4022
Nanjing University of Aeronautics and Astronautics, China

Ning Wu
Nanjing University of Aeronautics and Astronautics, China

Zain Anwar Ali
https://orcid.org/0000-0002-2143-2879
Sir Syed University of Engineering and Technology (SSUET), Pakistan

ABSTRACT

The evolution of internet of things (IoT) applications, cloud computing, smart cities, and 4G/5G wireless communication systems have significantly increased the demands for on-chip processing. Network on chip (NoC) is a viable alternative that can provide higher processing and bandwidth for increasing demands. NoC offers better performance and more flexibility with lower communication latency and higher throughput. However, use of NoC-based IoT devices have raised concerns on security and reliability of integrated chips (IC), which is used in almost every application. IoT devices share data that becomes vulnerable to attack and can be compromised during the data transfer. Keeping in view these security challenges, a detailed survey is presented that covers the security issues and challenges focusing on NoCs along with proposed countermeasures to secure on-chip communication. This study includes on-chip security issues for electrical as well as optical on-chip interconnects.

DOI: 10.4018/978-1-7998-1253-1.ch011
INTRODUCTION

The evolution of internet of things (IoT) inspires smart devices that are permeating in our lives, where smart services and applications are performing critical tasks that raise security concerns. Data proliferation is one of the critical issues, which designers and researchers are facing with the advent of IoT based smart cities projects (Samaila, Neto, Fernandes, Freire, & Inácio, 2018). With the increase in processing demand for IoT applications in every day of life, security and dependability have become key concerns while designing a network on chip based CMPs. Intellectual property (IP) hardware from third-parties are frequently used in order to reduce design time. The use of these IPs could cause leakage of data/information due to presence of some malicious Hardware Trojan (HT) (Basak, Bhunia, Tkacik, & Ray, 2017), (Tehranipoor & Koushanfar, 2010). The reason for information leakage may be unverified IPs, malicious foundry or untrusted design procedure. This problem of security lead researchers and designers to focus on security and reliability issues of on-chip interconnects (Bhunia et al., 2013). Network on Chip (NoC) has evolved as a practical solution that can provide future interconnection and processing requirements for IoT applications in chip multiprocessors (CMPs) (Bertozzi, Dimitrakopoulos, Flich, & Sonntag, 2015). In past, few works have been proposed to discuss security challenges in NoC based systems (Ben Achballah, Ben Othman, & Ben Saoud, 2017). However, more research needs to be accomplished for both electrical and optical NoC domains for secure on-chip communication. Figure 1 shows the IoT system setup with smart applications and services (Samaila et al., 2018).

As technology has exponentially evolved over the last few years, the number of cores on a single die has increased at a rapid pace, especially during the last decade. In this regard, the trend of technological developments in terms of increase in per chip core count, the increase in number of transistors, escalation in frequency and power consumption has been presented in form of trending plot titled “35 Years of Microprocessor Trend Data”, which has been initially presented by M. Horowitz et. al till 2010 (M. Horowitz, F. Labonte, O. Shacham, K. Olukotun, L. Hammond, and C. Batten, 2018). Later, the plots have been updated by K. Rupp from 2010-2017. It can be observed from the Figure 2 that the number of per chip cores is increasing with a power law. Since the number of transistors is increasing as per Moore’s Law, therefore chip count is increasing in form on-chip additional cores.

NoC based design has access to all the communication among different cores (Benini & De Micheli, 2002). Most of the work and research being done has recognized that NoC based architectures are suitable for secure on-chip communication. Since, components used in NoC architecture are homogeneous, taking that advantage designers have proposed several security mechanisms / schemes in an NoC based designs that provide better security than software approaches (Frey & Yu, 2017). Using hardware circuit among routers to secure data communication between different IPs is proposed in (Boraten & Kodi, 2018). Several threat models and countermeasures are proposed in literature to secure on-chip communication. Encryption and cryptographic algorithms are proposed in NoC links with additional area overhead and

Figure 1. Smart City Concept based on IoT System including smart applications of mobility, health and daily life
Related Content

**Energy-Efficient MAC Protocols in Distributed Sensor Networks**  
[www.igi-global.com/chapter/energy-efficient-mac-protocols-distributed/63553?camid=4v1a](www.igi-global.com/chapter/energy-efficient-mac-protocols-distributed/63553?camid=4v1a)

**Cooperative Error Control Mechanism Combining Cognitive Technology for Video Streaming Over Vehicular Networks**  
[www.igi-global.com/chapter/cooperative-error-control-mechanism-combining/77424?camid=4v1a](www.igi-global.com/chapter/cooperative-error-control-mechanism-combining/77424?camid=4v1a)

**DMT Optimal Cooperative MAC Protocols in Wireless Mesh Networks with Minimized Signaling Overhead**  
[www.igi-global.com/chapter/dmt-optimal-cooperative-mac-protocols/77410?camid=4v1a](www.igi-global.com/chapter/dmt-optimal-cooperative-mac-protocols/77410?camid=4v1a)

**Web Services for Healthcare Management**  
[www.igi-global.com/chapter/web-services-healthcare-management/63681?camid=4v1a](www.igi-global.com/chapter/web-services-healthcare-management/63681?camid=4v1a)