Mitigation of tampering attacks for MR-based thermal sensing in optical NoCs

Zhou, Jun; Li, Mengquan; Guo, Pengxing; Liu, Weichen

2020

Zhou, J., Li, M., Guo, P., & Liu, W. (2020). Mitigation of tampering attacks for MR-based thermal sensing in optical NoCs. 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). doi:10.1109/ISVLSI49217.2020.00009

<https://hdl.handle.net/10356/144232>

<https://doi.org/10.1109/ISVLSI49217.2020.00009>

© 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<https://doi.org/10.1109/ISVLSI49217.2020.00009>

Downloaded on 26 Apr 2023 19:15:00 SGT

Mitigation of Tampering Attacks for MR-based Thermal Sensing in Optical NoCs

Jun Zhou¹, Mengquan Li^{1,2}, Pengxing Guo^{1,3}, Weichen Liu¹

¹ School of Computer Science and Engineering, Nanyang Technological University, Singapore

² College of Computer Science, Chongqing University, Chongqing, China

³ School of Computer Science and Engineering, Northeastern University, Shenyang, China

Abstract—As an emerging role in on-chip communication, the optical networks-on-chip (ONoCs) can provide ultra-high bandwidth, low latency and low power dissipation for the data transfer. However, the thermo-optic effects of the photonic devices have a great impact on the operating performance and reliability of ONoCs, where the thermal-aware control is used to alleviate it. Furthermore, the temperature-sensitive ONoCs are prone to be attacked by the hardware Trojans (HTs) covertly embedded in the integrated circuits (ICs) from the malicious third-party components, leading to performance degradation, denial of service (DoS), or even permanent damages. In this paper, we focus on the tampering attacks on optical sampling during the thermal sensing process in ONoCs. Corresponding approaches are proposed to mitigate the negative impacts from HT attacks. Evaluation results indicate that our approach can significantly enhance the hardware security of thermal sensing for ONoC with trivial overheads of up to 3.06% and 2.6% in average latency and energy consumption, respectively.

Keywords—hardware security, thermal sensing, network-on-chip, micro-ring resonator, Trojan, tampering attack

I. INTRODUCTION

With the rising of design complexity and manufacturing costs of emerging many-processor systems, designers tend to utilize the devices or components from other vendors directly, i.e., the third-party intellectual property (3PIP), to fulfill the integration of the whole single facility [1]. However, these IPs can probably introduce some security risks [1, 2]. For instance, malicious or counterfeit circuits with hardware Trojans (HTs) will snoop or tamper the critical and sensitive data in the interconnection systems of the multi-processor systems-on-chip (MPSoCs). In fact, HTs in the compromising MPSoCs will result in data leakage, information manipulation, performance degradation, and denial of service (DoS), etc., inducing certain irreversible losses, such as systemic abnormal functions, or even permanent breakdown, which attracts more and more attention from both the academia and industry [1].

Many MPSoCs now employ electronic networks-on-chip (ENoCs) for inter-processor data transfers. As a traditional network-based communications subsystem in the integrated circuits (ICs), ENoC is a router-based packet switching interconnection among modules of SoC, applying the theories and methods of computer networks to on-chip communications and bringing notable improvements over conventional bus and crossbar architectures. In the meanwhile, recent progress in silicon photonics also has accelerated the integration of optical components with CMOS circuits in SoCs [3]. As a promising promotion to ENoCs, the optical networks-on-chip (ONoCs), especially those utilizing wavelength division multiplexing (WDM) technology [3, 4], can provide ultra-high bandwidth, low latency and power dissipation for modern many-processor systems. These advantages motivate the applications of ONoC for inter-processor communications.

However, both the communications in ENoC and ONoC need to face the challenges of overheating. The thermal issue impacts not only the network performance but also the chip

reliability. Higher temperatures will cause longer propagation delay, slower circuits switching, and larger leakage power [4]. As a result, for the ONoCs, which concern us more here, to reduce or eliminate the thermo-optic effects in interconnection has been one of the major research priorities [3]. Specifically, the temperature is a key indicator for the operation system (OS) to carry out the thermal-aware control of ONoCs through effective schemes, such as scheduling, mapping, and routing, etc., to avoid the hotspot and local overheat phenomena. The balance maintenance of on-chip temperature distribution guarantees the efficient communications of ONoCs.

Similar to an MPSoC with ENoCs, a many-processor system using ONoCs is expected to adopt the 3PIPs, which is vulnerable to security risks [2, 4]. The communication packets are probably to be snooped or tampered because of these unreliable IPs where HTs are embedded in ONoCs. On the other hand, many thermal sensing techniques are employed in the ONoCs to perform the thermal-aware control [4]. Similar to the communication packets, the sensing data obtained by thermal sensors may also be under leakage and manipulation attacks during its sampling and transmission. Consequently, OS will be cheated and misled seriously when the inaccurate on-chip temperature distribution is gained from the sensors, leading to the misjudgment of OS and induced inappropriate operations. Especially, tampering attacks are the primary security threats to cause the performance degradation, DoS of the core components in ONoCs, or even heat damage of the whole chip. Thus, efficient and effective mechanisms need to be proposed to accurately detect these HT attacks and recover the normal communications of ONoCs.

In this paper, for the first time to our knowledge, we propose an effective HT-mitigation method for the tampering attacks on data sampling of thermal sensing in ONoCs using optical sensors. The main contributions are as follows:

- We present a thermal sensing flow of ONoCs and an attack model therein. In this model, tampering attacks can be triggered by the counterfeit circuits within the control logic of the thermal sensor, which is based on the silicon micro-ring resonator (MR).
- A new anti-HT module is proposed to verify the data sampled from the thermal sensors based on the work flow and attack model. Retransmission operation will be applied until the relevant countermeasures work, ensuring the accuracy of the sampling data.
- Experimental results and analyses indicate that the proposed mitigation scheme provides security against tampering attacks from HTs with trivial overhead on latency, area, and energy consumption.

The rest of the paper is organized as follows: Section II introduces the preliminaries and related works; Section III presents the work flow and attack model; Section IV proposes the mitigation of the HT attacks in thermal sensing; Evaluation results are shown in Section V and Section VI concludes.

*E-mail: Jun Zhou (edo.zhou@ntu.edu.sg), Weichen Liu (liu@ntu.edu.sg)

II. PRELIMINARY AND RELATED WORK

A. Brief Background

1) ONoC Architecture

As illustrated in Fig. 1, a typical 2D-mesh ONoC is an optoelectronic hybrid network. Vertically in the upper layer of processor cores (i.e., processing elements (PEs)), an optical network (O-net) provides the optical interconnects between optical routers (O-routers) for inter-processor data transferring. And, an electronic network (E-net) consisting of electronic routers (E-routers) and metallic links lies in the under layer is to perform logical control.

Fig. 1. A typical 2D-mesh ONoC

2) Optical Thermal Sensor

In general, silicon MRs and optical waveguides perform the switching and transmission of optical signals, respectively. In Fig. 2(a), a single MR consists of one ring and two straight waveguides. Specifically, the optical signals from the *Input* port will be delivered to the *Through* port when the MR is configured to be switched *OFF*. Or else, the optical signals will get resonated into the ring and delivered to the *Drop* port if their wavelengths are in the range of resonant wavelength, while the signals whose wavelengths are beyond the range will be filtered. The cascaded MRs have been widely used as the basic optical filtering element (BOFE) at the receiver to demultiplex the WDM wavelengths (i.e., λ_i) before optical signals reach the photo-detectors (PDs), as demonstrated in Fig. 2(b). Also, the wavelength selectivity of MR leads itself naturally for WDM operations [3, 4]. With denser channel spacing than the normal WDM, dense wavelength division multiplexing (DWDM) is used to increase bandwidth over the existing fiber networks through combining and transmitting multiple signals simultaneously at different wavelengths on the same fiber. Generally, a typical DWDM system would use 40 channels with 100 GHz spacing, or 80 channels at 50 GHz spacing [4]. In this paper, we design the security mechanisms for thermal sensing in the DWDM-based ONoCs.

On the other hand, MR is highly sensitive to temperature variations (TVs) [5, 6]. The undesired mismatch between resonant wavelength and signal wavelength will lead to, because of TVs, additional optical power loss (indicated as ΔP , the same below) that can be converted to corresponding temperature data within a certain idle PE of the MPSoCs [5]. Thus, the inherent thermal sensitivity of MR makes itself an ideal choice of on-chip thermal sensing. Compared with the traditional electric thermal sensors, the MR-based type has several favorable features, such as compact size, robustness against mechanical shock, immunity to electro-magnetic interference, and well-modeled temperature dependence [6]. Although, the fabrication-induced process variation (PV), as

Fig. 2. Micro-ring resonator (MR) and cascaded MRs

well as the device-level wavelength tuning mechanisms, will introduce the challenges on accuracy and reliability of thermal sensing through MRs [7-9], it is sufficient for OS to obtain the temperature distribution on chip to execute the suitable thermal-aware control for the communications of ONoCs. [6] started to use an MR-based sensor to implement thermal sensing. In addition, [8] and [9] firstly utilized MRs to carry out the on-chip thermal sensing with resolving the challenges in accuracy and reliability, which arise from PVs, and local wavelength tuning.

B. Related Work

Due to the embedded malicious circuits with HTs, both ENoCs and ONoCs suffer from security issues nowadays. As surveyed in [1] and [2], previous works on hardware security in NoCs focused on different attacks & defenses patterns.

So far, the majority of existing security methods have been proposed for the ENoCs, which can be classified as follows: 1) **Detection and correction**. [10] gave us the packet-security (P-Sec) approach, a packet validation technique to protect compromised ENoC. Also, [11] provided the secure model checkers (SMCs) in the routers of a network under attack; 2) **Authentication**. [12] presented a progressive authentication scheme for the packets in third-party ENoC to avoid the tampering attack; 3) **Routing**. [13] secured ENoCs against timing attacks with non-interference based adaptive routing (NIBR). [14] first proposed an HT to misroute the packets, then presented a secure routing algorithm for run-time HTs detection and avoiding; 4) **Shuffling scheme**. [15] exploited error control schemes for transient and permanent HTs on ENoC links at run-time with link shuffling and isolation techniques, respectively. For [16], the authors designed an HT to compromise the crucial details of packets. A mitigation method based on a bit shuffling mechanism inside routers was proposed then; 5) **Obfuscation**. [17] presented a new light-weight target-activated sequential payload (TASP) HT model, and proposed a heuristic threat detection and several link obfuscation methods to avoid triggering of HTs. In [18], state obfuscation was applied to facilitate HT detection in the network interface (NI) of ENoCs. Furthermore, the authors of [19] and [20] combined the dynamic permutation and flit integrity check method to mitigate potential inside-router HTs inserted by attackers; 6) **Firewall or security module**. The authors of [21] presented a hardware firewall to secure the data transactions between ENoC routers. In [22], the ENoC firewall module is to check the physical addresses and reject untrusted requests from CPU to the memory. [23] described a low-overhead snooping invalidation module (SIM) in NIs of

ENoCs, and devised a snooping detection module, THANOS, to detect the malicious applications. Moreover, [24] proposed Prometheus, a drop-in solution inside NI in wireless NoC (WNoC, also a special type of ENoC); 7) **Mixed scheme.** [25] proposed an integrated run-time solution for both security and fault tolerance of FPGA-based SoCs with digital signatures, live monitoring, adaptive routing, and partial reconfiguration in an ENoC called X-Network. In [26], the authors offered Fort-NoCs, a series of techniques including data scrambling, packet certification, and node obfuscation to “cloud” the information obtained by attackers for defense.

Meanwhile, the specialized security approaches designed for ONoCs are still at an early stage. Since the traditional ONoC is an optoelectronic hybrid network, several security mechanisms proposed for ENoC can still be referred and applied. Whereas, the photonic components are also under the potential malicious attacks from different HTs. In [27] and [28], the authors presented the framework using key-based authentication signatures along with the architecture-level enhancements to protect the packets in communications of ONoCs from data-snooping HTs.

According to the current relevant research status, in this paper, the security issues in ONoCs are our primary concerns here. *So far, in addition, nearly all the relevant works are concentrated on the attacks and defenses of sensitive data packets transmitted in the networks.* But similarly, the on-chip temperature distribution we care about is also prone to be “obfuscated” because of its tight relationship with the network control [4]. *Actually, however, there is scarcely any research aiming at this domain.* It is indeed necessary to present an effective and targeted mitigation approach for HT attacks in thermal sensing of ONoC due to the great impacts of thermo-optic effects on the performance and reliability of photonic devices. Moreover, the relevant attacks from HTs may occur in either the optical or electronic components of ONoC. Therefore, we need to alleviate the passive influences induced in the respective parts.

III. WORK FLOW AND ATTACK MODEL

A thermal sensing flow in ONoC and our attack model are demonstrated in this section to introduce the related operations on the thermal sensing data, and the corresponding attack scenarios created by the triggered HTs.

A. Thermal Sensing Flow

As no specific thermal sensing flow with MR-based sensor has been provided before [6-9], we present one in this section for ONoC of the classical 2D-mesh topology in Fig. 3. For the normal communications, generally, the *optical circuit switch* is applied in ONoC for routing. An electronic “*path-setup*” packet will be sent to E-router from NI while communications are in need between two PEs. When the packet arrives, the E-router will inject it to the E-net, and attempt to establish an optical path for the data transmission. Specifically, according to the routing information contained in the packet header, the E-routers internally mark the associated resources in ONoC as “reserved” after receiving the feedbacks from the destination nodes, and activate the corresponding basic optical switching elements (BOSEs) in the connected O-routers to establish an optical path. Along the optical path, bulk data can be delivered end-to-end without halfway buffering and arbitration.

For our thermal sensing scenario, the O-router is a core device to collect the temperature-related data. In general, an

MR-based thermal sensor of ONoC is comprised of three core components: a multi-wavelength laser source, a BOFE, and multiple PDs, as shown in Fig. 4. The MRs in the BOFE filter out their own designated resonant wavelengths from the input ones, demultiplexing the W wavelengths before the optical signals reach respective PDs. For a single MR, we can derive a predicted temperature value based on the temperature dependence of MRs formulated in [7] and [8], which model the relation between the thermal-induced ΔP of an MR and its ambient temperature. Here, the temperature values cannot be gained directly through the MR-based sensors actually. The relevant data including ΔP of MR will be transferred to the corresponding E-router from the *sampling node* through NI’s packetization with an extra metallic link, as shown in Fig. 3. Then, in the E-net, the router will route the received data to the *collection node*, an “idle” PE, to carry out the temperature calculation and centralized control, since the access latency through the shared memory is extremely high [7]. This PE is designated by OS for the load balancing of ONoCs, which is the criteria to specify the *collection node* dynamically and periodically with a moderate interval. In our design, the ΔP transmission is based on E-net, as the temperature sampling should not affect normal optical communications.

Fig. 3. An example of thermal sensing flow in traditional 2D-mesh ONoC

B. Attack Model

According to the provided thermal sensing flow in ONoCs mentioned above, some serious kinds of HT attacks can be triggered by the counterfeit circuits. Prior researches [10-28] seldom concentrated on the control information, but the data packets of networks. Generally, for the thermal-aware process, there are two potential HT attack scenarios during this flow in the compromised O-net and E-net, i.e., attacks during the sampling and transmission, respectively. In this paper, we focus on the former one, as no related studies before.

As described in [7] and [8], the thermal sensitivity of MRs can be abstracted as Eq. 1, which describes the relationship between the ΔP of an ON-state MR at the *Drop* port and its ambient temperature, T .

$$T = T_0 + [(\sqrt{\alpha \cdot c^{\Delta P} - \beta} + \Delta\lambda) / \rho_{MR}] \quad (1)$$

where the temperature-dependent resonant wavelength shift coefficient of the MR, i.e., ρ_{MR} , is a constant as well as α , β and c according to the specific MR, T_0 denotes the nominal operating temperature (typically the usual indoor temperature, i.e., 25°C), and $\Delta\lambda$ represents the known change of resonant wavelength due to the PV of MR. The related calculations for T will be carried out in the idle PE where all the ΔP -loaded packets arrive. Here, because the MR-based sensor we adopt is applied to implement thermal sensing without participation in optical communications, no consideration is needed for local wavelength tuning. Generally, eight MRs are contained in one thermal sensor for relatively accurate temperature value via average calculation [6-8]. Thus, as demonstrated in Fig. 3,

the sampling sensing data including all the ΔP values is to be collected and delivered from the *sample node* to the *collection node* via the E-routers on the path with red arrows.

Fig. 4. One MR-based thermal sensor with HTs for ONoCs

By applying the modulation voltage (MV) on an MR, its resonance wavelength will be changed, which improves the flexibility and robustness of MR for DWDM operations. Note that, the non-linear relationship between ΔP and MV of the electronic control logic is offered in [29]. However, in Fig. 4, the HTs embedded in control logic will actually manipulate the actual value of MV, resulting in the incorrect ΔP , then finally the wrong temperature value. $V_1, V_2, V_3, \dots, V_w$ are the output MVs generated from the control logic for each MR in the sensor [30]. In fact, they can be easily transformed by utilizing a direct current (DC) chopper [31] or even a simple DC voltage regulator (e.g., voltage divider) at a negligible overhead for just a series of extra resistors, diodes, and capacitors, which is easy to deploy while hard to notice for testers. In general, the HT takes up less than 5% of the area of the compromised module [12, 23, 26]. Once the chopper or regulator is triggered by an internal activation code, the original MV values will be manipulated.

Besides, the relevant counterfeit circuits of HTs can be activated to perform a persistent attack or intermittent attack, which brings different effects to the MV values, and makes itself more difficult to be detected and mitigated. Efficient response measures need to be proposed to find out which ΔP values are inaccurate and correct them properly by carrying out specific counteracting modifications.

IV. MITIGATION OF HT ATTACKS IN THERMAL SENSING

Here, we propose an HT-mitigation scheme based on the work flow and attack model above. The relevant functions are integrated together to constitute a whole functional module for the mitigation of HTs, i.e., MHT, which is embedded in NI, as shown in Fig. 5. Considering the key role of NI in the thermal-aware control flow of ONoC, it is a suitable module to execute the anti-HT mechanism, while not adding extra overhead to the on-chip interconnections. For MHT, the optic-checker module is deployed for the checking of obtained ΔP values transferred from O-router to NI in ONoCs, and the feedback module is in charge of providing the related feedbacks on the adjustment approach to send to the MR control logic for reference. According to the thermal sensing flow in Fig. 3, the network data will be transmitted between O-/E-router and NI in packet (P) format. And sampling info will be sent in flit (E) format from E-router to the NI of the *collection node*, as it is delivered in the wormhole-routing-based E-net.

Actually, ΔP value is mainly affected by MV, TV, and PV of an MR together. Note that, normally, the eight MRs in an optical thermal sensor have different fabrication parameters, i.e., the PV of individual MR is different from each other. As PV is a known value to us, we can calculate its corresponding

Fig. 5. Attack mitigation for the malicious circuits in ONoCs

“impact” on ΔP [7-9, 32]. On account of the same temperature change for all MRs in one sensor, the impact that ΔP of each MR obtains under TV is also the same. Besides, the possibility which all the MRs are under attack simultaneously in one thermal sensor is extremely low. For instance, even though the activation probability of the HT in an MR’s control logic can reach 50% or so, the probability of the scenario that the HTs in all eight MRs’ control circuits are triggered is less than 0.4%. However, in fact, all of these control logics are still potentially under attack simultaneously no matter how small the probability is. For explanation, in one sensor, we mark a certain ΔP value as the standard one, i.e., ΔP_S , whose selection criteria will be given later in this section. And, ΔP_A is used to indicate the ΔP value of MR under severer attack. The relevant ΔP data is marked in Eq. 2 and 3, respectively.

$$\Delta P_S = \Delta P_S^{MV} + \Delta P_S^{TV} + \Delta P_S^{PV} \quad (2)$$

$$\Delta P_A = \Delta P_A^{MV} + \Delta P_A^{TV} + \Delta P_A^{PV} \quad (3)$$

where ΔP^{MV} , ΔP^{TV} , and ΔP^{PV} indicate the specific ΔP values affected by MV, TV, and PV. As described above, ΔP_S^{PV} and ΔP_A^{PV} are both available. In addition, the TVs of MRs within one thermal sensor are the same according to our scenario, i.e., $\Delta P_S^{TV} = \Delta P_A^{TV}$. Hence, ΔP^{TV} values will be eliminated through the operation of subtraction between ΔP_S and ΔP_A . Then the difference of these two ΔP values will be only dependent on the ΔP^{MV} -based expression. Above all, if all the ΔP^{MV} values of the MRs are equal, then no HT is embedded or activated, or the attack effect for each MR is the same. Once there is at least one ΔP^{MV} value that is different from ΔP_S^{MV} , it is indicated that this sensor must be attacked. Also, according to the relationship between the transmissivity at modulation wavelength and MV of the thermal sensor [29], we fit an approximate function as Eq. 4 through certain functions [33] using MATLAB Curve Fitting Toolbox and a convincing photonic integrated circuits simulator INTERCONNECT of Lumerical [34, 35].

$$f(x) = [(e^{ax-b})/(e^{cx-d} + 1)] + q \quad (4)$$

where a, b, c, d , and q are constant coefficients. The curve of the function in Eq. 4 is described in Fig. 6 for the ideal MR without PV. While for actual MR, all the constant coefficients

need to be adjusted accordingly. Besides, by reason of $\Delta P^{MV} = 10 \cdot \lg(f(x))$ [7, 8], we can figure out the malicious variation of MV, then inform the corresponding control logic to modify the output MV to a reasonable value for sensor to retransmit the correct data by tolerating the attacks inside, e.g., adjusting the input voltage of the affected part of control logic circuits. Whether the tampering attack is persistent or intermittent, our strategy checks out the ΔP values when receiving them from PDs of the BOFE. The retransmission will not stop until the effective modifications are applied for MVs of MRs.

Fig. 6. Transmissivity at modulation wavelength over MV for an ideal MR

Note that, we choose the ΔP with the lowest specific ΔP^{MV} value as ΔP_S in one sensor. The reason is that, as mentioned, ΔP^{MV} is the only possibly attacked variable among the eight ΔP values, and the value “1” should be normally obtained by the calculation of the transmissivity at modulation wavelength as close as possible so as to resonate the particular optical signals, while letting ΔP^{MV} be closer to “0”. That is, generally, ΔP^{MV} of a certain MR should be “0” if its MV is not tampered. Here, we set $\Delta P_S^{MV}=0$ for related calculations. Even if the HTs in all of the control logics of MRs are activated rarely, causing that any ΔP^{MV} value of the eight MRs cannot be equal to “0”, we still adopt the lowest ΔP^{MV} value to be the standard one. It is because this value is the closest one to “0”, guaranteeing the most approximate accuracy of the temperature distribution of the whole chip for coordination and control of OS.

V. EVALUATION AND ANALYSIS

A. Evaluation Setup

We modified a full system simulator Gem5 [36] and a cycle-accurate NoC simulator Booksim [37] to model the ONoC of $m \times n$ 2D-mesh topology. And, each of the tile [38] consists of an x86 processor core based on out-of-order (OoO) execution and an SRAM cache in 22 nm process technology. The detailed system configurations are described in Table I for the performance and overhead evaluations. Benchmark suite of PARSECv2.1 [39] is utilized with Gem5 to evaluate the proposed HT-mitigation method with real applications. We also validated the simulator in terms of energy consumption and area according to the estimated results obtained from the NoC simulator and DSENT tool [40].

As most of the attack model and network architecture of related works are widely different with ours, we present a comparison between the baseline ONoC (without any security mechanisms) and the proposed attack-mitigation variant for investigation. Besides, the persistent and intermittent attacks are set to be launched randomly from the activated HTs.

B. Performance Study

Transmission latency of the packets is a key indicator for the performance analysis of the HT-mitigation approaches for the whole ONoCs, where we employ the PARSEC benchmark

TABLE I. FULL-SYSTEM SIMULATION CONFIGURATIONS

Processing Element	$m \times n$ processor cores, 2GHz, 4 issue, x86, 32KB, 2-way I-cache/D-cache (1-cycle latency)
L2 Cache	Private, 256KB, 4-way, 8-cycle latency
ONoC Topology	$m \times n$ 2D-mesh, XY routing
Memory	4GB DRAM, 1 rank, 1 channel, 8 banks, 90-cycle latency
Coherence Protocol	MOESI protocol
O-router	DWDM supported, 8 MRs per thermal sensor, Cygnus architecture [41]
E-router	3 pipeline stages, wormhole flow control, 8-flit depth buffer, 2 virtual channels

suite as the workload in an 8×8 mesh network. Fig. 7 presents the packet latency normalized to the latency of respective corresponding baseline networks with different ratios of activated HTs (i.e., 5%, 10%, 15%, and 20%, the common cases in practice [1]). For the comparison, the performances of secure ONoCs are lower because of the ΔP -checking and retransmission operations, etc.

Fig. 7. Latency comparison with different ratios of triggered HTs

Specifically, for the high-contented applications here, such as *canneal* and *freqmine*, the packet latency increment is relatively large. But, for the low-contented applications, e.g., *streamcluster*, the increment is moderate. In conclusion, the higher the ratio of activated HTs is, the higher the extra latency will be introduced. E.g., the latency rises 4.22% maximally and 3.06% on average with 20% of HTs triggered, which is still acceptable for the ONoC to employ the security-enhanced thermal-aware communications at a relatively low cost. The performance will degrade significantly if the ratio of triggered HTs rises continuously, which will be detected/classified and reported to OS to take the subsequent actions, such as the logical isolation and physical replacement for related modules or devices under attack.

C. Overhead Analysis

1) Area Footprint

An MR-based thermal sensor occupies 0.0123 mm^2 of silicon area that is similarly sized to most of the CMOS-compatible electric ones compared in [9]. And, the area of MHT is $52.65 \text{ } \mu\text{m}^2$ (also smaller than the two typical security enhancement modules in [10] and [26], as shown in Table II) with 1.03% extra area for a NI. As the NI area occupies less than 10% of a tile [38] consisting of PE, NI, router and other relevant links, the increase of the tile area will be much smaller than 1%, which is negligible.

TABLE II. AREA FOOTPRINT OF DIFFERENT NOC SECURITY ENHANCEMENT MECHANISMS

P-Sec [10]	Fort-NoCs [26]	Proposed MHT
300~12850 μm^2	4917 μm^2	52.65 μm^2

2) Energy Consumption

The energy consumption of our sensor is just 627.71 pJ/Sa [9], which is much lower than those of electric sensors. As illustrated in Fig. 8, the comparison on energy consumption, which is normalized to the respective corresponding baseline ONoCs, for different scales of mesh networks (i.e., 6×6 , 8×8 , 10×10 , and 12×12) with activated HTs at 15% ratio is shown. For a relatively large-size network, for instance, it is indicated that the energy consumption rises 3.81% maximally and 2.6% on average in the 12×12 mesh ONoC. For the scalability study, the power growth rates are still in a reasonable scope with an overall slow convergence trend. Though the absolute number of activated HTs increases, which results in more possible overhead on extra control and communications because of the ΔP -checking and retransmissions, while the overall energy consumption (both the static and dynamic parts) will rise far more rapidly after the network size reaches a certain level according to the relevant configurations.

Fig. 8. Energy consumption comparison in networks at different scales

VI. CONCLUSION AND FUTURE WORK

In view of the potential tampering attacks to the thermal-aware control of ONoCs from the malicious HTs, we thus present an attack model applied during the data sampling in the thermal sensing flow of ONoCs, and then propose an HT-mitigation scheme to alleviate the passive impacts. Evaluation results indicate that our approach is an attractive security-enhanced solution for thermal-aware management in ONoCs with trivial overheads of up to 3.06% and 2.6% in average latency and energy consumption, respectively.

In fact, the snooping and tampering attacks within E-net during the electronic transmission for thermal sensing are also needed to be concerned. Moreover, The detection of the whole ONoC statuses is essential to be applied to report to OS for preventing the further negative impacts from the HT attacks. We will be concentrated on these two aspects to implement reliable, scalable, and lightweight security enhancements for the optoelectronic networks of different topologies.

ACKNOWLEDGEMENT

This work is partially supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 2 (MOE2019-T2-1-071) and Tier 1 (MOE2019-T1-1-072), and Nanyang Technological University, Singapore, under its NAP (M4082282) and SUG (M4082087).

REFERENCES

- [1] Z. Huang, et al., "Hardware Trojan: research progress and new trends on key problems," in *Journal of Computers*, 42(5), 2019, pp. 993-1017.
- [2] L. Daoud, "Secure network-on-chip architectures for MPSoC: overview and challenges," in *Proc. of MWSCAS*, 2018.
- [3] D. A. B. Miller, "Device requirements for optical interconnects to silicon chips," in *Proc. of IEEE*, 97(7), 2009, pp. 1166-1185.
- [4] K. Bergman, et al., "Photonic network-on-chip design," 1st edition, Vol. 68,

- Springer, 2014.
- [5] H. T. Kim et al., "Cascaded ring resonator-based temperature sensor with simultaneously enhanced sensitivity and range," in *Optics Express*, 24(9), 2016, pp.9501-9510.
- [6] W. Liu, et al., "Quantitative modeling of thermo-optic effects in optical networks-on-chip," in *Proc. of GLSVLSI*, 2017.
- [7] M. Li, "Hardware-software collaborative thermal sensing in optical network-on-chip based manycore systems," in *ACM TECS*, 2019.
- [8] W. Liu, et al., "Thermal sensing using micro-ring resonators in optical network-on-chip," in *Proc. of DATE*, 2019.
- [9] M. Li, "Lightweight thermal monitoring for optical networks-on-chip via router reuse," in *Proc. of DATE*, 2020.
- [10] T. Boraten, et al., "Packet security with path sensitization for NoCs," in *Proc. of DATE*, 2016.
- [11] T. Boraten, et al., "Secure model checkers for network-on-chip (NoC) architectures," in *Proc. of GLSVLSI*, 2016.
- [12] M. Hussain, "Runtime detection of hardware Trojan in untrusted network-on-chip," A thesis for the degree of Ph.D. in *UNSW, Australia*, 2018.
- [13] T. H. Boraten, et al., "Securing NoCs against timing attacks with non-interference based adaptive routing," in *Proc. of NOCS*, 2018.
- [14] L. Daoud, et al., "Routing aware and runtime detection for infected network-on-chip routers," in *Proc. of MWSCAS*, 2018.
- [15] Q. Yu, et al., "Exploiting error control approaches for hardware Trojans on network-on-chip links," in *Proc. of DFTS*, 2013.
- [16] M. K. JYV, et al., "Run time mitigation of performance degradation hardware Trojan attacks in NoC," in *Proc. of ISVLSI*, 2018.
- [17] T. Boraten, et al., "Mitigation of denial of service attack with hardware Trojans in NoC architectures," in *Proc. of IPDPS*, 2016.
- [18] J. Frey, et al., "Exploiting state obfuscation to detect hardware Trojans in NoC network interfaces," in *Proc. of MWSCAS*, 2015, pp. 1-4.
- [19] J. Frey, et al., "A hardened network-on-chip design using runtime hardware Trojan mitigation methods," in *Integration*, 56, 2017, pp. 15-31.
- [20] M. Hussain, et al., "A non-invasive approach to detect and mitigate hardware Trojan in network on chip," in *IJCSMC*, 8(7), 2019, pp. 188-202.
- [21] A. B. Achballah, et al., "Toward on hardware firewalling of networks-on-chip based systems," in *Proc. of IC_ASET*, 2017.
- [22] M. D. Grammatikakis, et al., "High-level security services based on a hardware NoC firewall module," in *Proc. of WISES*, 2015.
- [23] V. Y. Raparti, et al., "Lightweight mitigation of hardware Trojan attacks in NoC-based manycore computing," in *Proc. of DAC*, 2019.
- [24] B. Lebednik, et al., "Architecting a secure wireless network-on-chip," in *Proc. of NOCS*, 2018.
- [25] T. Wehbe, et al., "Secure and dependable NoC-connected systems on an FPGA chip," in *IEEE Trans. on Reliability*, 65(4), 2016, pp. 1852-1863.
- [26] D. M. Ancajas, et al., "Fort-NoCs: mitigating the threat of a compromised NoC," in *Proc. of DAC*, 2014.
- [27] S. Pasricha, et al., "Securing photonic NoC architectures from hardware Trojans," in *Proc. of NOCS*, 2018.
- [28] S. V. R. Chittamuru, et al., "SOTERIA: exploiting process variations to enhance hardware security with photonic NoC architectures," in *Proc. of DAC*, 2018.
- [29] A. Ayazi, et al., "Linearity of silicon ring modulators for analog optical links," in *Optics Express*, 20(12), 2012, pp. 13115-13122.
- [30] Z. Li, et al., "Aurora: a cross-layer solution for thermally resilient photonic network-on-chip," in *IEEE TVLSI*, 23(1), 2015, pp. 170-183.
- [31] A. Adam, et al., "A novel multilevel DC chopper supplying DC motor," in *Proc. of ICEDSA*, 2016.
- [32] P. Guo, et al., "Fault-tolerant routing mechanism in 3D optical network-on-chip based on node reuse," in *IEEE Trans. on Parallel and Distributed Systems*, 31(3), 2020, pp.547-564.
- [33] J. Han, et al., "The influence of the sigmoid function parameters on the speed of backpropagation learning," in *Proc. of IWANN*, 1995.
- [34] MATLAB Curve Fitting Toolbox, <https://www.mathworks.com/products/curvefitting.html>.
- [35] INTERCONNECT, <https://www.lumerical.com/products/interconnect/>.
- [36] N. Binkert, et al., "The gem5 simulator," in *SIGARCH Comput. Archit. News*, 39(2), 2011, pp. 1-7.
- [37] N. Jiang, et al., "A detailed and flexible cycle-accurate network-on-chip simulator," in *Proc. of ISPASS*, 2013.
- [38] S. R. Vangal, "An 80-tile sub-100-w teraflops processor in 65-nm CMOS," in *IEEE Journal of Solid-State Circuits*, 43(1), 2008, pp. 29-41.
- [39] C. Bienia, et al., "The PARSEC benchmark suite: characterization and architectural implications," in *Proc. of PACT*, 2008.
- [40] C. Sun, et al., "DSENT - a tool connecting emerging photonics with electronics for opto-electronic networks-on-chip modeling," in *Proc. of NOCS*, 2012.
- [41] R. Ji, "Five-port optical router based on microring switches for photonic networks-on-chip," in *IEEE Photonics Technology Letters*, Vol. 25, No. 5, 2013, pp. 492-495.