Thermo-Attack Resiliency: Addressing a New Vulnerability in Opto-Electrical Network-on-Chips

Mahdi Hasanzadeh*, Meisam Abdollahi†, Amirali Baniasadi†, Ahmad Patooghy*
*Department of Computer Systems Technology, North Carolina A&T State University, NC, USA
†Department of Electrical & Computer Engineering, University of Victoria, Victoria, Canada

2024 25th International Symposium on Quality Electronic Design (ISQED) | 979-8-3503-0927-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISQED60706.2024.10528773

***Abstract*—Optical Network-on-Chip (ONoC) has recently emerged as a power- and latency-efficient solution to improve the performance of Multi-Processor System-on-Chips (MPSoCs). ONoCs utilize optical communications to transfer a bulk of data with significantly reduced energy consumption compared to their electrical counterparts. However, the temperature sensitivity of optical routers might be exploited by adversaries to conduct thermal attacks on the optical components of such MPSoCs. In this paper, for the first time, we exploit this vulnerability and define three variations of a thermal attack on optical and electro-optical MPSoCs. The proposed attack alters the functionality of an MPSoC by inducing a range of malicious activities, including 1) Packet misdelivery, drops, and losses; 2) Data errors in normal and secure packets; and 3) Putting the network in a deadlock situation. In addition to defining the thermal attack, the paper proposes the application of stochastic source routing to protect MPSoCs against thermal attacks. This approach enhances the security of MPSoCs by making it challenging for the adversary to identify and track packets. Our evaluations validate the effectiveness of the proposed countermeasure.**

***Index Terms*—Opto-electrical network on chip, Thermal variation, Security, Routing algorithm, Microring resonator**

I. Introduction

It has been widely accepted that Multi-Processor System-on-Chips (MPSoCs) can benefit from Electronic Network-on-Chips (ENoCs) as their communication backbone [1]. The ENoCs utilize packet-based data exchange between on-chip routers, which interconnect modules of the SoC. This architecture significantly improves upon conventional bus and crossbar architectures by applying computer network theories and methods to on-chip communications [2]. However, recent technology advancements have stimulated the integration of optical components within SoCs i.e., the emergence of Optical Networks-on-Chips (ONoCs) [3]. The optical counterpart offers ultra-high bandwidth, low latency, and low power dissipation, all of which make ONoCs a promising alternative to ENoCs [4]. Some serious challenges of ONoCs include overheads for optical/electrical conversions, laser integration complexities, reliability challenges, and security concerns [5], [6]. The hybrid opto-electrical NoC seems to be an interesting solution for achieving the benefits of both technologies while alleviating their disadvantages [7], [8].

From the security point of view, both ENoC and ONoC face the challenge of thermal and process variations [9], [10]. These fluctuations that might happen naturally can have a notable impact on the NoC's performance affecting key metrics such as communication latency, throughput, and energy consumption. For example, as the chip's temperature rises, both network delay and network leakage power increases, and communication channels' bandwidth degrades [9], [11]. Thermal fluctuations can also occur intentionally due to some malicious intentions i.e., Hardware Trojans (HTs) can be used to conduct such intentional fluctuations in MPSoCs [12], [13]. HTs may come with third-party intellectual property (IP) modules developed by other vendors [14] during the integration phase of MPSoCs. Although HTs are capable of doing a range of malicious activities i.e., data leakage, information manipulation, and denial of service [15], in our case of interest, HTs can snoop on and manipulate thermal information on the chip [16].

In this paper, for the first time, we use temperature variations as a security vulnerability in order to attack hybrid opto-electrical NoCs. We show that the vulnerability can be misused by an adversary to hijack the network and steal sensitive information. Then, leveraging the special characteristics of these topologies, we propose a novel solution to protect hybrid opto-electrical NoCs against the proposed attack. The main contributions of the paper are as follows:

- We identify a novel security vulnerability for hybrid opto-electrical network on chips. The vulnerability takes advantage of the electrical component of the chip to implement a novel attack on the optical routers of the chip, manifesting in three different scenarios.
- We introduce a novel countermeasure based on a stochastic source routing that hides the generator's information to protect against one of the attack scenarios. The proposed countermeasure works with the encrypted destination information to address the other two scenarios.

The remainder of this paper is organized as follows. Section II discusses the background of network model, optical data transmission, and security threats of hybrid NoCs. Section III discusses the thermal variation used in the proposed thermal attack. Section IV reviews how the proposed method can be used as a countermeasure. Section V presents simulation

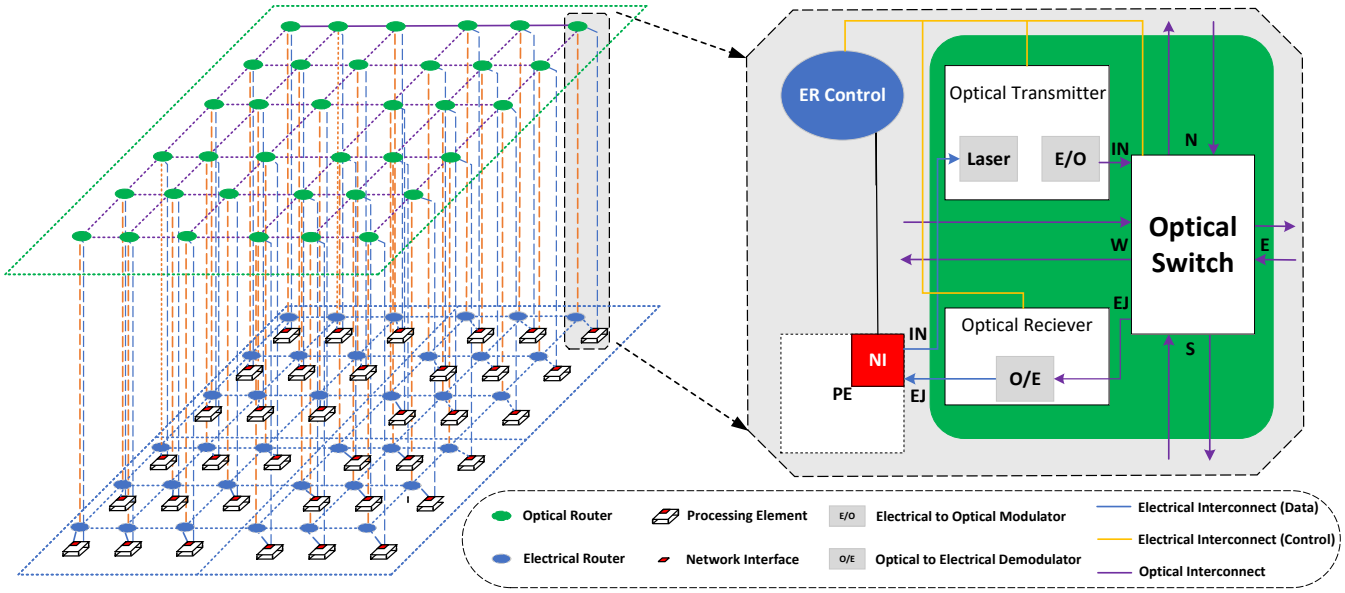


Fig. 1: Cluster-based hybrid opto-electrical on-chip network

experiments and analyzes the results obtained. Section VI summarizes the related works and Section VII concludes the paper.

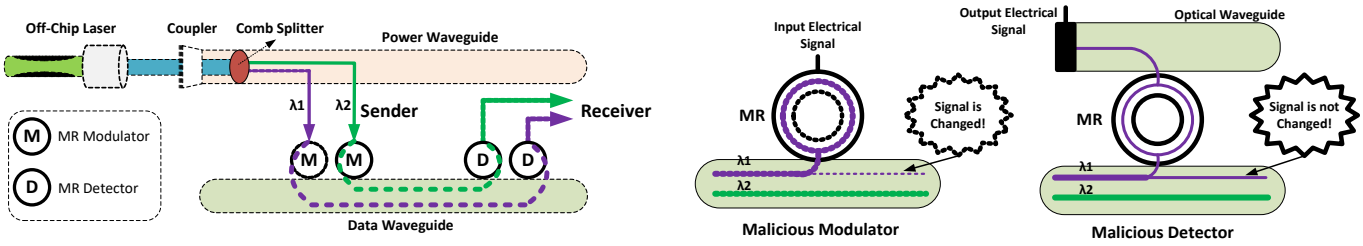
II. Background

Combining the advantages of electrical and optical data transmission has led to the emergence of hybrid opto-electrical NoC. According to the architecture shown in Figure 1, long-distance (inter-cluster) communications take place through optical channels, while electrical communications are used for local destinations (intra-cluster) [7], [8], [17], [18]. In the electrical domain, packet switching is applied, while in the ONoC domain, optical circuit switching is used. When communication is needed between two PEs, NI will send a "path-setup" packet to the electrical router. Upon receiving this packet, the electrical router injects it into the electrical network and establishes an optical path for later data transmission whenever an optical path is required. Optical paths allow bulk data to be sent end-to-end without the need for intermediary buffers, arbitration, or other processing. Optical signals are modulated at a specified wavelength(s) e.g., Microring Resonators (MRs) are a commonly employed example, wherein optical signals are modulated using electrical signals. In this modulation, an array of photodetectors converts the optical signals into equivalent electrical signals after they have been multiplexed into a single optical waveguide [19]. In this paper, we follow the cluster-based hybrid architecture of Figure 1 at which optical routers are connected based on a mesh-based Crux optical router with modifications for Dense Wavelength Division Multiplexing (DWDM)-enabled network [20].

In MR technology, the resonant wavelength is highly sensitive to the thermal condition of the chip. To mitigate the effects of temperature and fabrication-induced variations, microring resonators require tuning by applying external current or heat (thermal tuning) to the MRs. This process allows for the adjustment of their effective refractive index [21]. MRs are tuned electrically and/or thermally in ONoCs through a separate tuning circuit (Figure 2a). A similar circuit can be used to turn on and turn off the MRs as needed. However, such tuning circuits are the most vulnerable part of the device when it comes to the security of the chip. For instance, the tuning circuit can be altered by malicious hardware (i.e., an HT), to tamper with the resonant wavelength of ring resonators. An example of a malicious MR is shown in Figure 2b at which the malicious MR is partially turned on. In this scenario, the malicious modulator will draw some power (or the entire power) from the wavelength of the data carrying signal. This will lead to corrupted data since optical '1's can be altered into '0's due to power loss. Alternatively, the malicious detector (Figure 2b) can be tuned to filter out only a small part of the passing wavelength and drop it on the photodetector to dump the data. In this way, the waveguide data continues to travel to its target detector for legitimate communication despite the small amount of filtered power. The data from the waveguide can be snooped by malicious detector MRs without being altered, thus posing a major threat to photonic links.

To be more accurate, according to Equation 1, when an optical stream is passed through an MR, its phase shift is a multiple of 2π [22].

$$m \times \lambda_{MR} = 2\pi R \times n_{eff} \quad (1)$$



(a) On-chip optical transmission

(b) Malicious or malfunctioned modulator/detector MR

Fig. 2: DWDM optical data transmission and the threat of malicious/malfunctioned MR

where λ_{MR} is known as the vacuum resonant wavelength, R is known as the bending radius of the ring, n_{eff} is known as the effective index of the resonator, and m is a positive integer constant. Based on the initial resonant wavelength at the nominal operating temperature, i.e., T_0, the relation between the resonant wavelength of an MR and the ambient temperature can be stated as Equation 2.

$$\lambda_{MR} = \lambda_0 + \rho_{MR} \times (T - T_0) \tag{2}$$

where ρ_{MR} is the coefficient of the MR's resonant wavelength shift that varies with temperature. ρ_{MR} can be measured by the Equation 3 where in this equation, for example, the approximate value of n_g for optical waveguides at $1,550nm$ is 4.63.

$$\rho_{MR} = \frac{(\lambda_0 \times \delta n_{eff})}{n_g} \tag{3}$$

δn_{eff} is the thermo-optic coefficient of effective refractive index, which is lower than silicon refractive index [23]. The authors of [11] have shown that MR resonant wavelength is linearly related to temperature variation. According to Equation 3, a $5nm$ in resonance wavelength shift occurs as a result of a $55°C$ temperature change. As the number of channels increases in DWDM systems, the thermal impact becomes more significant as the wavelength width of each channel decreases. Also, as the temperature increases between 300K and 400K, the optical power loss of an MR increases monotonically [24].

III. The Proposed Thermal Attacks

In this section, we explore how the thermal vulnerabilities of ONoCs can be exploited in various scenarios to compromise users' privacy. For this purpose, we executed deliberate attacks using the Access Noxim [25] simulator. The network under consideration consists of two layers: the first layer is an electrical network, and the upper layer is an optical network.

According to our evaluations detailed in this section, an adversary can conduct the thermal attack according to any of the following three scenarios to either drop or steal the data which is labeled private. The root of the attack is the thermal sensitivity of ONoCs (described in Section II). According to the proposed attack model, the attack agent tries to overload an area of the network to overheat certain optical routers, in order to shift the routers' working wavelength. Such intentional congestion serves the attacker to conduct wavelength changes on the optical routers, enabling access to data that the altered router was not meant to otherwise. The following scenarios focus on how the thermal vulnerability can be exploited to compromise the security and reliability of ONoCs.

- **NACK Replay (Attack Scenario-1):** An attacker attempts to pinpoint the information's source and deploys some NACK packets to the designated source router. This NACK replay attack is based on the fact that the NoC implements a handshake process in an end-to-end manner. The NACK replay will lead to a rise in network traffic within the designated area, potentially increasing the local or overall chip temperature. Ultimately, this elevated temperature can trigger a wavelength change in the victim ONoC routers.
- **Packet Drop (Attack Scenario-2):** If the attacker cannot locate the source address of a packet, they may devise to drop a portion of the packet to force the destination to send a NACK to the source, i.e., the application of a fault injection attack to conduct the ONoC thermal attack.
- **False Traffic Injection (Attack Scenario-3):** The attacker can directly work on injecting massive false traffic to break or congest an area of the network to violate the thermal boundaries of the victim ONoC router(s).

We conducted system-level simulations to study the feasibility of the attack scenarios mentioned above. Figure 3 illustrates the temperature changes in the optical layer of an 8×8 network, which is being attacked under Attack Scenario-1. In this instance, we executed a 4600-cycle thermal attack (Scenario-1) on the optical layer of a hybrid network. It is notable to mention that we have not done any tampering with the optical layer, we only conducted NACK replays in the electrical layer and recorded the temperature profile of the optical layer accordingly. The results demonstrate that the attack can increase the temperature of the network to a large extent, resulting in the wavelength change in the optical routers.

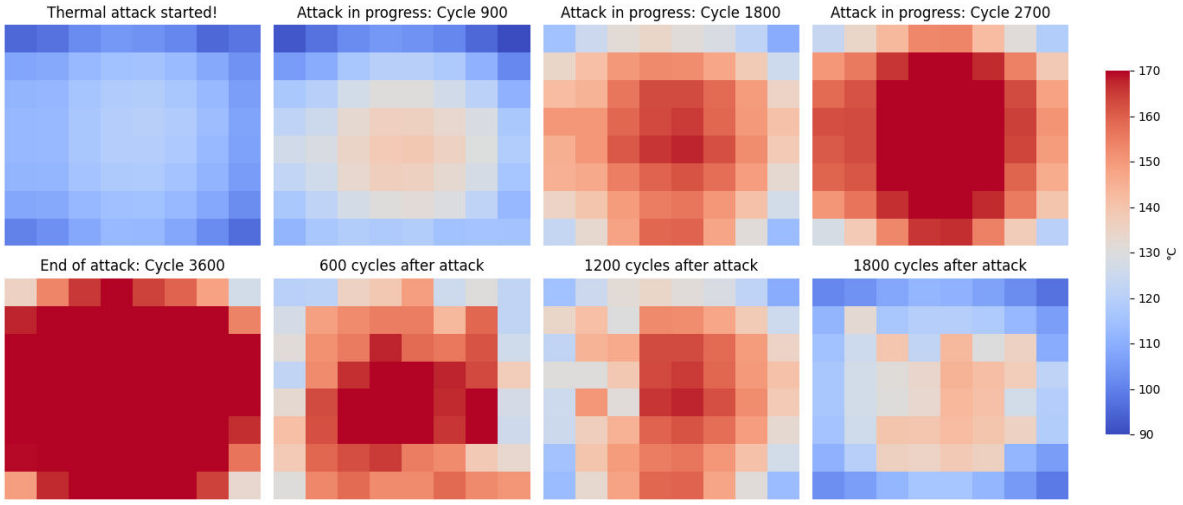


Fig. 3: Temperature variation during approximately 4600 cycles of attack conducted on an 8×8 network under a moderate traffic rate

TABLE I: Temperature profile of the chip during the attack

Traffic Type	ΔT during attack ($^\circ C$)		Average temperature during attack ($^\circ C$)
	Minimum	Maximum	
Low	17	38	114
Moderate	24	55	127.5
High	38	160	171.65
Very High	47	210	209.83

TABLE II: Observed outcomes of the thermal attack on the baseline network

Attack	Traffic	Packet Drop	Data Error	Mis-Delivery	Packet Loss	Deadlock
Scenario-1 6x6	Low	57	1341	43	38	2
	Moderate	79	1575	69	72	3
Scenario-2 6x6	Low	43	1182	39	41	3
	Moderate	57	1379	91	83	4
Scenario-3 6x6	Low	50	998	46	40	2
	Moderate	64	1256	70	79	5
Scenario-1 8x8	Low	29	870	30	20	1
	Moderate	37	1439	61	46	3
Scenario-2 8X8	Low	26	826	29	37	2
	Moderate	41	1335	78	51	5
Scenario-3 8x8	Low	30	981	34	59	3
	Moderate	49	1016	59	67	4

In Table I, the temperature profile of a whole chip has been collected during the attack. The two first columns show the minimum and maximum temperature variation, and the last column is the average temperature of the whole chip. We have repeated the thermal attack for the other two scenarios and observed the same outcome, i.e., significant wavelength shift in optical routers. The attack has affected the network significantly as reported and summarized in Table II, where we attacked 6×6 and 8×8 networks with a duration of 5000 and 7000 cycles, respectively. The data is collected for low and moderate traffic conditions. In the rest of this section, we discuss the observed results and the outcomes of the performed attacks under each scenario.

Outcome-1 (Packet Loss): If the packet's type is tampered with during an attack[1], it can result in one of the two outcomes. Firstly, the tampered packet might be dropped from the network as routers may not recognize the packet's type. This case was observed in the 6×6 network i.e., 38 cases of packet loss under the low traffic condition. As the size of the network increases, more packets may be at risk of such a drop as a result of the thermal attack. Secondly, the packet may get stuck in the buffers of NoC routers and occupy the buffers indefinitely. As we show later, this outcome may lead to congested areas in the network and increase the power/thermal profile of the chip.

Outcome-2 (Mis-delivery): If the attack tampers the destination address field of a packet, the packet will be forwarded in the wrong path and will be delivered to a wrong core (we called this situation packet mis-delivery). Although such packets eventually exit the network, the actual application that is waiting for them will never receive them. According to the logs shown in Table II, we have observed 34 packet mis-delivery cases for the 8×8 network when we conducted the attack in a 7000-cycle period.

Outcome-3 (Data Error): The most common outcome of a thermal attack is the tampering of the body of packets, which can lead to errors in non-control data flits of packets. In Table II, it is shown that this is the most frequent outcome of the attack, with significant numbers of data errors observed in various experimental settings.

Outcome-4 (Fake Packet): Assume a packet consists of 10 flits: 1 header, 8 data, and 1 trailer flit. If one of the data flits (say the 5^{th} flit) is tampered with by a thermal attack so that its type changes from data into a header, then the network

[1]The packet type information is stored in the header of each packet

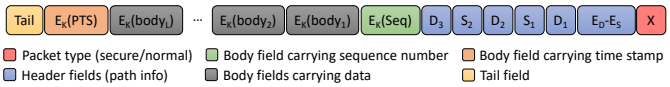


Fig. 4: The format defined for secure packets allows stochastic source routing without having source and destination information within the packets

will treat the second part of the packet (flits 5 to 10) as a new packet. This means that the original packet will now be divided into two incomplete packets, each with a length of 5 flits. Interestingly, our experiments have confirmed that attackers could achieve this rare condition by executing thermal attacks.

Outcome-5 (Global Deadlock): If the attacker has the opportunity to enforce a good number of lost packets or create some fake packets, some flits may remain un-handled in buffers of the NoC, meaning that the flits occupy the buffers indefinitely. If the number of such flits increases, they may end up in a global deadlock that infects all parts of the network.

IV. Countermeasures

In this section, we discuss our proposal to address the thermal vulnerability and its related attack scenarios. The main idea here is to utilize a stochastic source routing methodology that routes messages stochastically among a number of routing options. This countermeasure, indeed, hides the packets' routing information, preventing attackers from conducting a successful thermal attack, as they will not be able to identify the target optical router. The effective feature of the countermeasure is that it adjusts the chances of selecting alternative routes depending on the network condition, response time, and thermal and security profile of the routes.

A. Stochastic Secure Routing

Using stochastic source routing, packets can choose from some routes to reach the destination node based on their security profile [26], [27]. The secure packet header, illustrated in Figure 4, contains crucial information guiding the packet's traversal and handling. Beginning with a single bit denoted as X_{bit}, it identifies whether the packet is secure or non-secure. Encrypted within the E_D field is the destination address, crucial for anonymous routing, with further details to be elaborated later. Traversal directions are specified in fields D_1 to D_3, encompassing options such as X^+, X^-, Y^+, Y^-, and *OPTIC*. Additionally, the fields $S1$ and $S2$ indicate the number of strides necessary to navigate the packet to its first and second turns. The encrypted sequence number, represented by $E_K(Seq)$, further secures packet integrity. Encryption for various fields, including E_D, $E_K(Seq)$, $E_K(body)$, and $E_K(PTS)$, employs a pre-shared key K via a symmetric-key encryption scheme. A secure packet will be routed stochastically among XY[2], YX, or optical paths using secure routing. The probability of picking alternate routes is stored in three registers which will be updated as needed[3]. Initially, for inter-cluster communications, optical routes are given a higher probability than other routing algorithms.

By the selected strategy, the shortest path will be calculated and embedded in the header of a secure packet. The source and destination addresses of a secure packet are not disclosed within the path information. To maintain packet security and prevent the exposure of source and destination details, three routing alternatives (so-called $L1$, $L2$, and $L3$ paths) are available for secure packets. The probability of selecting each route (respectively, P_{L1}, P_{L2}, and P_{L3}, where $P_{L1}+P_{L2}+P_{L3}=1$) is used by the path computation algorithm shown in Algorithm 1. According to this process, which takes place at the network interface unit of each router, a path will be computed and stored in the header of a secure packet. The three routing options for secure packets are detailed below.

1) ***L*1 Path:** Packet headers include a ***XY*** path toward the destination with turn-last through the electrical layer. These types of packets will remain in the electrical network until they reach their destination.
2) ***L*2 Path:** The ***YX*** path to the destination with turn-first is embedded in the packet's header meaning that the packet starts its path through the ***Y*** direction.
3) ***L*3 Path:** A wavelength-based circuit-switched optical path through the optical layer. Secure packets will be ejected to the ***Optical*** network if the path is selected and will be injected into the electrical network when the destination is reached by the peer optical router.

As outlined in Algorithm 2, the packet type is set, and the source (E_S) and destination (E_D) addresses are encrypted, updating the corresponding fields in the packet. In line 3, the algorithm computes the horizontal, vertical, and layer differences between the source and destination nodes. The algorithm then employs a stochastic selection process to select one of the three routing alternatives to generate the path.

Path generation for $L1$ and $L2$ includes both real and misleading turns, while $L3$ generates a path that may contain either a misleading turn or a path through the optical network. In the $L1$ subroutine (lines 6-12), S_1, D_1, and D_2 are computed deterministically based on the source and destination coordinates. However, S_2 and D_3 are chosen randomly to mislead potential attackers regarding the packet's destination.

$L2$ (lines 13-20) follows a similar concept but gives priority to vertical movement over horizontal. Conversely, in $L3$ (lines

[2]In XY routing, the packet initially takes channels of the X direction. Upon reaching the destination column, it makes a turn and continues in the Y direction. The YX routing works oppositely.

[3]Information from thermal sensors, packet waiting times, and security priority is used to update the probabilities.

Algorithm 1 Secure Routing

Input: Strides S_1, S_2, Directions D_1, D_2, D_3;
Input: Encrypted Source & Destination Address E_S;
Input: Encrypted Destination Address E_D;
Input: Router Address R;
Output: Selected Output Channel $Out_{Channel}$;

if $(E_D == E_R)$ **then**
  $Out_{Channel} = Local$;
else
  Set $Next_{VC} = Current_{V_C}$; #1 for XY, 2 for YX and 3 for Optical packets.
  if $(S_1 \neq 0)$ **then**
    $S_1 \leftarrow S_1 - 1$; and $Out_{Channel} = D_1$;
  else if $(S_2 \neq 0)$ **then**
    $S_2 \leftarrow S_2 - 1$; and $Out_{Channel} = D_2$;
  else
    $Out_{Channel} = D_3$; # After reaching the peer optical router, the packet will be ejected from the Optical Network to its destination.
  end if
end if
Return; =0

21-22), the packet is directly sent to the optical network, and the variable m, representing the number of hops to the peer optical router destination, is initialized. This approach increases the likelihood of bypassing a malicious router in the electrical router's path if the conditions are favorable for choosing this route.

B. Deadlock Freedom

The incorporation of optical routing for secure packets in its raw form can create a cyclic dependency between NoC buffers. To avoid this issue, we have devised two virtual channels (VC), namely VC_1 and VC_2, with specific allocation policies, same as mentioned in [26]. Both VCs are available for normal packets at the source. However, once assigned to a VC, a normal packet cannot switch between the two VCs during its journey. The allocation of VCs to normal packets is based on the traffic conditions at the source node. For secure packets, the routing algorithm enforces specific restrictions when acquiring VCs, depending on the routing scenario adopted for each secure packet. Secure packets are allocated to VCs based on the following policies.

- When a packet travels through a secure path designated as XY, it is limited to using only VC_1. To enforce this policy, the source node initiates the transmission of the packet into the network with VC_1. Once assigned, this VC, it will be used for the entire journey of the secure packet.
- A secure packet with path YX uses only VC_2 until destination. Likewise, this policy is enforced by the network interface unit at the time of path computation.

Algorithm 2 : Secure Path Computation

Input: Source & Destination Address Plaintext P_s, P_d;
Output: Encrypted Source & Destination Address E_S, E_D;
Output: Strides S_1, S_2, Directions D_1, D_2, D_3;
Output: Packet type X_{bit};

$X_{bit} \leftarrow 1$;
$E_D \leftarrow HB\text{-}2(P_d)$;
$\Delta X = P_d.X - P_s.X$; and $\Delta Y = P_d.Y - P_s.Y$;
Set $Current_{V_C} = 1$; # Initial VC for all paths except YX
Goto L1, L2, or L3 with a probability distribution of P_{L_1}, P_{L_2} and P_{L_3} s.t. $P_{L_1} + P_{L_2} + P_{L_3} = 1$;
L1: (an XY path) # Path with real and misleading turns
$S_1 \leftarrow abs(\Delta X)$;
$S_2 \leftarrow Rand(n)$; and $D_3 \leftarrow Rand(X^+, X^-)$; # To mislead the attacker
if $(\Delta X \geq 0)$ **then**
  $D_1 \leftarrow X^-$; **Else** $D_1 \leftarrow X^+$;
end if
if $(\Delta Y \geq 0)$ **then**
  $D_2 \leftarrow Y^-$; **Else** $D_2 \leftarrow Y^+$;
end if
Return;
L2: (a YX path) # Path with real and misleading turns
$S_1 \leftarrow abs(\Delta Y)$;
$S_2 \leftarrow Rand(n)$; and $D_3 \leftarrow Rand(Y^+, Y^-)$; # To mislead the attacker
Set $Current_{V_C} = 2$; # Initial VC for YX path
if $(\Delta Y \geq 0)$ **then**
  $D_1 \leftarrow Y^-$; **Else** $D_1 \leftarrow Y^+$;
end if
if $(\Delta X \geq 0)$ **then**
  $D_2 \leftarrow X^-$; **Else** $D_2 \leftarrow X^+$;
end if
Return;
L3: (an Optical path) # The path contains an optical route
$m \leftarrow RandBetween(0, \Delta OP - 1)$;
$S_1 \leftarrow abs(\Delta OP) - m$; # Takes the remaining m hops once ejected from the optical network
Return;

TABLE III: Observed outcomes of the thermal attack on the protected network

Attack	Traffic	Packet Drop	Data Error	Mis-Delivery	Packet Loss	Deadlock
Scenario-1 6x6	Low	0	0	0	0	0
	Moderate	0	0	0	0	0
Scenario-2 6x6	Low	0	0	0	0	0
	Moderate	6	79	0	3	0
Scenario-3 6x6	Low	0	0	0	0	0
	Moderate	8	106	6	7	0
Scenario-1 8x8	Low	0	0	0	0	0
	Moderate	0	0	0	0	0
Scenario-2 8X8	Low	0	0	0	0	0
	Moderate	1	21	3	6	0
Scenario-3 8x8	Low	0	0	0	0	0
	Moderate	5	137	8	6	0

- A secure packet that uses an optical route starts its journey on VC_1 and continues along this route until it reaches the second turn, which is the turn from Y to X. At this point, the packet needs to switch over to VC_2. This means that the packet switches to VC_2 when it returns to the direction of X, where its actual destination is located.

V. Results and Discussion

To assess the effectiveness of the proposed security countermeasure, we conducted two types of experiments. First, we used the Access Noxim NoC simulator to simulate the behavior of a NoC-based MPSoC equipped with our proposed method. The results of this experiment are presented in the following two subsections.

A. Security Evaluation

We conducted network-level simulations to evaluate the security of the system against these attack scenarios. According to our countermeasure (see Section IV), packets in the simulation environment are divided into two types: secure and non-secure. Secure packets use a method specified in their header to determine their route, whereas non-secure packets are routed deterministically using XY or YX. The simulation is conducted on 8×8 and 6×6 networks with a second optical layer, over 100,000 cycles with a 10% warm-up period. The delay for the optical link is calculated using a formula that can be found in [17]. Table II shows the effectiveness of the countermeasures against attacks for each scenario. As it can be seen from Table III, the proposed countermeasure successfully protects the network against the introduced thermal attack under all possible scenarios. We believe that this level of success is achieved due to the following behaviors of the proposed stochastic source routing: 1) if an adversary attempts to resend the message from the same source, its packets will be routed through different paths, thus reducing the attacker's control over the attack area; 2) if a path becomes congested or experiences a high thermal profile, the routing gives it less chance to be used; and 3) proposed countermeasure prevents attackers from identifying the source of a packet, that enhances protection against the NACK attacks.

TABLE IV: Area and dynamic power consumption overheads of the proposed security system compared to the baseline router and the baseline 16-core MPSoC

		Silicon Area (μm^2)	Dynamic Power (μW)
Baseline	Baseline (Router)	65,972.70	268.5
	Baseline (16-Core MPSoC)	1769364.2	2704.6
Stochastic Source Routing	Proposed (Router)	85,263.50	428.9
	Overhead w.r.t Baseline (Router + NI)	**29%**	**159.7%**
	Proposed (16-Core MPSoC)	1,799,443.30	3017.1
	Overhead w.r.t Baseline (16-Core MPSoC)	**1.7%**	**11.6%**

B. Network Performance Evaluation

Performing a thermal attack on the network can have a significant impact on network performance in both normal and secure modes. In the case of a 6×6 network, the average delay can be observed in Figure 5a, while for an 8×8 network, it is shown in Figure 5b. Our proposed method prioritizes the transmission of secure packets, resulting in a reduction in the average delay of secure packets, as depicted in Figure 5.

C. Hardware Evaluation

Our proposed method was verified using Verilog HDL and synthesized with synopsis DesignCompiler™ tool to estimate its hardware overhead. This tool uses 45nm Nangate library ASIC technology. In our design, the baseline NoC consists of four virtual channels per physical channel, each with a depth of eight buffers and a 32-bit data width. To implement the proposed system, the NI and router of the MPSoC have been modified to include the components as listed below.

- In order to maintain a secure path for packets that use secured source routing, a module has been implemented in each router. With this module, the router can divide packets into two types - secure and normal. Subsequently, the packets are routed using a specified routing algorithm discussed in Section IV.
- Three registers at each router hold the probability of each path for future routings of secure packets. Routing scenarios for the source routing will be updated based on this module.

The hardware synthesis results for a 16-core MPSoC are shown in Table IV. The first tab displays the baseline router and MPSoC for 16-Core without any additional components. The second tab shows the overall architecture outcome along with the suggested security system. As shown in the table, the area overhead of the securing system affects the router by a 29% increase, and the dynamic power of that router is increased by 159.7%. Our security system has just 1.7%

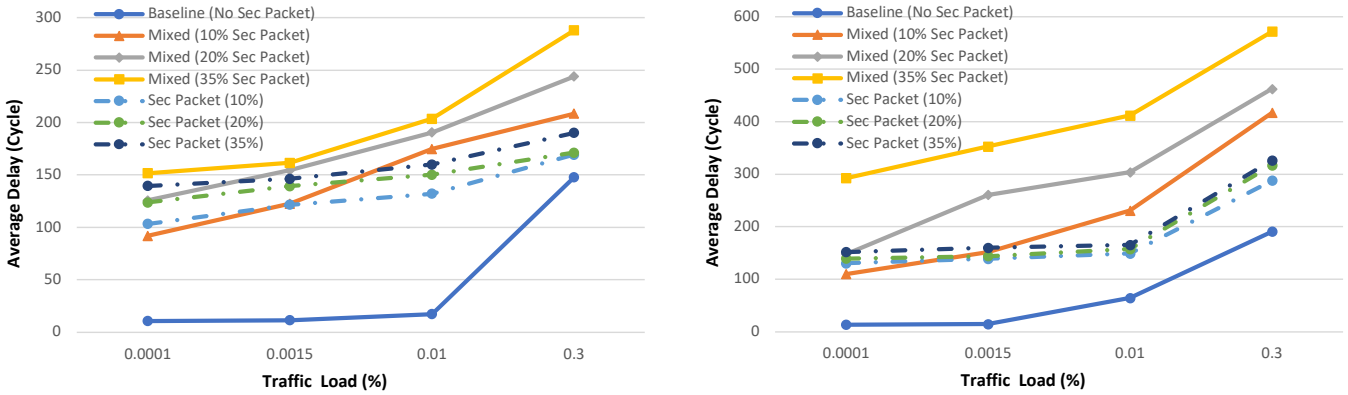


Fig. 5: Average network latency of secure packets, non-secure packets, and combined for (a) 6×6 and (b) 8×8 networks under different rates of secure packets

overhead according to the whole MPSoC, and this increase is about 11% for dynamic power.

VI. Related Work

The authors in [28] discussed several security challenges in NoC design across electrical, wireless, and photonic domains, along with some promising solutions. An overview of remote denial of service attacks caused by hardware Trojan insertion and timing channel attacks was presented in [29]. Furthermore, they showed that two types of remote attacks can also be effective in PNoCs. A hybrid wavelength and mode division multiplexing PNoC was also designed for the first time, along with countermeasures to protect against threat models. Additionally, new potential threats that might affect the 3D PNoC safety were discussed.

Rani et al. [30] implied that by using a high-power signal, an attacker can inject a gain competition attack into ONoCs. This attack aims to deprive legitimate signals of amplification, thereby initiating a gain competition attack in ONoCs. As a security threat to ONoCs, gain competition attacks have been investigated for the first time in their proposed approach. A model of the attack was developed and its effects on the performance of optical NoC were analyzed. They also proposed strategies for detecting attacks and countermeasures for mitigating them. A new end-to-end security protocol was created by Bashir et al. [21] for on-chip optical networks that is impervious to replay, eavesdropping, and message spoofing attacks. Their scheme also exploited optical network properties to reduce the effect of cryptographic operations' long latency.

ONoCs are vulnerable to hardware Trojans that manipulate electrical driving circuits to cause MRs to spy data from neighboring wavelength channels of a shared photonic waveguide. This introduces a serious security threat. The SOTERIA framework was presented by Chittamuru et al. [31], which offers a way to protect data in PNoC architectures from snooping attacks using process variation-based authentication signatures. DWDM-based PNoCs can be enhanced with reservation-assisted security enhancements at the architecture level. Based on crossbar-based PNoC architectures, the authors in [32] combined circuit- and architecture-level schemes into SOTERIA framework. Zhou et al. in [24], [33] examined tampering and snooping attacks during thermal sensing through micro-ring resonators in ONoCs. In ONoCs, they studied tampering and snooping attacks during thermal sensing through micro-ring resonators. To verify and protect thermal sensor data for attacks using optical sampling and electronic transmission, a new structure for the anti-HT module was proposed based on the workflow and attack model provided. To further enhance the high-level control of the security statuses of the networks, the authors developed a detection scheme based on spiked neural networks (SNNs).

VII. Conclusion

Hybrid opto-electrical Network-on-Chip combines optical and electrical communication technologies to facilitate high-speed data transfer and reduce power consumption. The hybrid approach leverages the strengths of both optical and electrical communication while addressing their respective limitations. However, the thermal sensitivity of optical components in a hybrid system can be exploited, posing security risks to the chip. This paper, for the first time, studies the feasibility of such thermal attacks on hybrid Network-on-Chips. We introduced three variations of the thermal attack and observed a wide range of severe outcomes from the conducted attack. Additionally, the paper proposes a novel routing methodology to mitigate the attack. The proposed routing makes stochastic decisions based on the network's security profile and thermal condition to protect the chip against thermal attack. In our future work, we intend to investigate and identify the attack behaviors under synthetic and real-world traffic using

machine learning models. We anticipate that this study, along with future expansions, will draw further attention from the community to the security challenges of opto-electrical chips.

VIII. Acknowledgement

This research has been partially supported by the National Science Foundation under award number 2302537.

References

[1] S. Kundu and S. Chattopadhyay, *Network-on-chip: the next generation of system-on-chip integration*. Taylor & Francis, 2014.

[2] I. A. Alimi, R. K. Patel, O. Aboderin, A. M. Abdalla, R. A. Gbadamosi, N. J. Muga, A. N. Pinto, and A. L. Teixeira, "Network-on-chip topologies: Potentials, technical challenges, recent advances and research direction," *Network-on-Chip-Architecture, Optimization, and Design Explorations*, 2021.

[3] H. Mekawey, M. Elsayed, Y. Ismail, and M. A. Swillam, "Optical interconnects finally seeing the light in silicon photonics: Past the hype," *Nanomaterials*, vol. 12, no. 3, p. 485, 2022.

[4] K. Bergman, L. P. Carloni, A. Biberman, J. Chan, and G. Hendry, "Photonic network-on-chip design," 2014.

[5] I. G. Thakkar, S. Pasricha *et al.*, "Libra: Thermal and process variation aware reliability management in photonic networks-on-chip," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 4, no. 4, pp. 758–772, 2018.

[6] M. Baharloo, M. Abdollahi, and A. Baniasadi, "System-level reliability assessment of optical network on chip," *Microprocessors and Microsystems*, vol. 99, p. 104843, 2023.

[7] G. Kurian, J. E. Miller, J. Psota, J. Eastep, J. Liu, J. Michel, L. C. Kimerling, and A. Agarwal, "Atac: A 1000-core cache-coherent processor with on-chip optical network," in *Proceedings of the 19th international conference on Parallel architectures and compilation techniques*, 2010, pp. 477–488.

[8] M. Abdollahi, A. Namazi, and S. Mohammadi, "Clustering effects on the design of opto-electrical network-on-chip," in *2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP)*. IEEE, 2016, pp. 427–430.

[9] B. Li, L.-S. Peh, and P. Patra, "Impact of process and temperature variations on network-on-chip design exploration," in *Second ACM/IEEE International Symposium on Networks-on-Chip (nocs 2008)*. IEEE, 2008, pp. 117–126.

[10] M. Mohamed, Z. Li, X. Chen, L. Shang, and A. R. Mickelson, "Reliability-aware design flow for silicon photonics on-chip interconnect," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 8, pp. 1763–1776, 2013.

[11] Z. Li, M. Mohamed, X. Chen, E. Dudley, K. Meng, L. Shang, A. R. Mickelson, R. Joseph, M. Vachharajani, B. Schwartz *et al.*, "Reliability modeling and management of nanophotonic on-chip networks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 1, pp. 98–111, 2010.

[12] A. Sarihi, A. Patooghy, P. Jamieson, and A.-H. A. Badawy, "Hardware trojan insertion using reinforcement learning," in *Proceedings of the Great Lakes Symposium on VLSI 2022*, ser. GLSVLSI '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 139â142.

[13] R. JS, K. Chakraborty, and S. Roy, "Hardware trojan attacks in soc and noc," *The Hardware Trojan War: Attacks, Myths, and Defenses*, pp. 55–74, 2018.

[14] S. Charles and P. Mishra, "A survey of network-on-chip security attacks and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1–36, 2021.

[15] P. Mishra and S. Charles, *Network-on-chip security and privacy*. Springer, 2021.

[16] L. Daoud, "Secure network-on-chip architectures for mpsoc: Overview and challenges," in *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2018, pp. 542–543.

[17] M. Abdollahi, Y. Firouzabadi, F. Dehghani, and S. Mohammadi, "Thamon: Thermal-aware high-performance application mapping onto opto-electrical network-on-chip," *Journal of Systems Architecture*, vol. 121, p. 102315, 2021.

[18] S. Jamilan, M. Abdollahi, and S. Mohammadi, "Cache energy management through dynamic reconfiguration approach in opto-electrical noc," in *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. IEEE, 2017, pp. 576–583.

[19] J. Bashir, E. Peter, and S. R. Sarangi, "A survey of on-chip optical interconnects," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–34, 2019.

[20] M. Nikdast, J. Xu, L. H. K. Duong, X. Wu, X. Wang, Z. Wang, Z. Wang, P. Yang, Y. Ye, and Q. Hao, "Crosstalk noise in wdm-based optical networks-on-chip: A formal study and comparison," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 11, pp. 2552–2565, 2014.

[21] J. Bashir, C. Goodchild, and S. R. Sarangi, "Seconet: a security framework for a photonic network-on-chip," in *2020 14th IEEE/ACM International Symposium on Networks-on-Chip (NOCS)*. IEEE, 2020, pp. 1–8.

[22] Y. Ye, J. Xu, X. Wu, W. Zhang, X. Wang, M. Nikdast, Z. Wang, and W. Liu, "System-level modeling and analysis of thermal effects in optical networks-on-chip," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 2, pp. 292–305, 2012.

[23] M. Li, W. Liu, N. Guan, Y. Xie, and Y. Ye, "Hardware-software collaborative thermal sensing in optical network-on-chip–based manycore systems," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 18, no. 6, pp. 1–24, 2019.

[24] J. Zhou, M. Li, P. Guo, and W. Liu, "Attack mitigation of hardware trojans for thermal sensing via micro-ring resonator in optical nocs," *ACM Journal of Emerging Technologies in Computing System*, vol. 17, no. 3, pp. 1–23, 2021.

[25] I. Access, "Lab (2018). access noxim."

[26] A. Patooghy, M. Hasanzadeh, A. Sarihi, M. Abdelrehim, and A.-H. A. Badawy, "Securing network-on-chips against fault-injection and crypto-analysis attacks via stochastic anonymous routing," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 19, no. 3, pp. 1–21, 2023.

[27] A. Sarihi, A. Patooghy, M. Hasanzadeh, M. Abdelrehim, and A.-H. A. Badawy, "Securing on-chip communications: An on-the-fly encryption architecture for socs," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2021, pp. 741–746.

[28] S. Pasricha, J. Jose, and S. Deb, "Electronic, wireless, and photonic network-on-chip security: Challenges and countermeasures," *IEEE Design & Test*, 2022.

[29] P. Guo, W. Hou, L. Guo, Z. Cao, and Z. Ning, "Potential threats and possible countermeasures for photonic network-on-chip," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 48–53, 2020.

[30] K. Rani, H. Weerasena, S. A. Butler, S. Charles, and P. Mishra, "Modeling and exploration of gain competition attacks in optical network-on-chip architectures," *arXiv preprint arXiv:2303.01550*, 2023.

[31] S. R. Chittamuru, I. Thakkar, V. Bhat, and S. Pasricha, "Soteria: Exploiting process variations to enhance hardware security with photonic noc architectures, 2018 55th acm," in *ESDA/IEEE Design Automation Conference (DAC),(San Francisco, CA, 2018)*.

[32] S. Pasricha, S. V. R. Chittamuru, I. G. Thakkar, and V. Bhat, "Securing photonic noc architectures from hardware trojans," in *2018 Twelfth IEEE/ACM International Symposium on Networks-on-Chip (NOCS)*. IEEE, 2018, pp. 1–8.

[33] J. Zhou, M. Li, P. Guo, and W. Liu, "Mitigation of tampering attacks for mr-based thermal sensing in optical nocs," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2020, pp. 554–559.