Hardware Attack Models in Tiled Chip Multi-Core Processors: A Survey

Nilanjana Das, Friedrich Pauls, Mattis Hasler, Sebastian Haas, Nils Asmussen
Barkhausen Institut, Dresden, Germany
{first name.last name}@barkhauseninstitut.org

***Abstract*—An increasing number of use of third-party IP participation along with the growing need for sophisticated Tiled Chip Multi-Core Processor systems (TCMP) led to vulnerability exploitation in the integrated circuit (IC) supply chain, primarily the insertion of hardware Trojans (HTs). The HTs are malevolent alterations made to genuine designs to compromise IC performance. In this study, we first evaluate the most recent HT attack models in TCMPs, emphasizing the targeted platform, the supply chain's risk level, and then a discussion based on our findings. We classify the HT attack models according to the targeted platforms in TCMP, like processor, caches, network interface, router, and virtual channel allocator.**

***Index terms* – Hardware Trojans, Hardware Security and Threats, Tiled Chip Multi-Core Processor (TCMP), Attack Models, Countermeasures.**

I. Introduction

The semiconductor industry has experienced unparalleled growth due to technological advancements, which has led to an increase in the complexity of circuits created on a single chip. System-on-Chip (SoC) is a new design technique developed by design engineers to keep up with such advanced degrees of integration. Multiprocessors System-on-Chip (MPSoC) [1] is a method to build a high performance platform by packing a processor die with numerous smaller processing units (PEs) for clock frequency scaling and high throughput systems. The Tiled Chip Multi-Core Processor (TCMP) is a type of System-on-a-Chip (SoC) intended for parallel systems with large amounts of data. The Network-on-Chip (NoC) [2] is an interconnection network that facilitates communication between many tiles hosted on a chip. Each tile in a TCMP has processors, cache memories, and a network interface. Every tile shares an equal portion of a Last Level Cache (LLC).

Although the advantage provided by the TCMP for integrating multiple processors is worthwhile, modern MPSoCs are still in risk due to numerous security related attacks. In recent days the TCMPs have become more complex due to the involvement of heterogeneous tiles which involve numerous processing elements like accelerators, RISCV, GPU, etc. [3].

In order to meet the requirements and time-to-market constraints, TCMP manufacturers have started depending on the third party intellectual property Cores (3PIP) for outsourcing parts of the design [4]. These practices put the design at risk for a number of security flaws, such as the presence of Hardware Trojans (HT) or other malicious circuits [5]–[7].

In order to initiate attacks like data leakage, illegal access, functional faults, and delay-of-service, HTs are incorporated

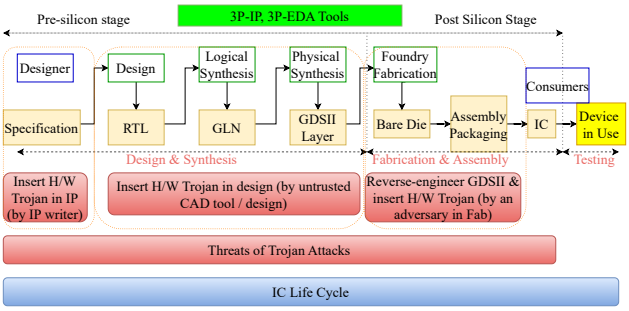

Fig. 1: HT attack scenarios in different phases of IC life cycle

in an Integrated Circuit (ICs) to modify the behavior of the system [8]. IC manufacturing depends on many multi-entity supply chain process which includes design, synthesis, fabrication, assembly, and testing phases. From the past decades research on HTs have discovered that the attack can take place in almost any IC manufacturing phase which is shown in Figure 1. Some research works considers HT attack in the design phase [9]–[14]; whereas some works are primarily focused on HTs for the 3PIP and Computer Aided Design (CAD) tool phase like [15], [16], while some works [17]–[23] presents the HT vulnerabilities for fabrication and test phase. Concerns about the vulnerabilities due to HT and the resultant compromise of system security have been expressed globally [24]–[26] especially since recent discoveries point to feasibility of such attacks [27]–[29]. Moreover, several unexplained military mishaps in the past have been attributed to the presence of malicious hardware modifications [5], [30].

There are different kind of existing HT design mechanisms [31], [32] available based on the physical, activation, and action characteristics; externally and internally activated, digital (combinational/ sequential) HTs, analog HTs etc. Since TCMP is composed of different parts like processors, caches, network interface (NI), NoC, router, and virtual channel allocator, its complexity has increased and becomes prone to HT attacks.

There exist many works that mainly survey the HT attacks and defences [6], [32]–[35]. Some recent studies are focused on the impact of HT attack models on NoCs [36], [37], wireless NoCs [38], Internet of things (IoT) [39], [40], cyber physical systems (CPS) [41], and MPSoCs [42]. In contrast to the existing works, this work provides a novel categorization of the HTs based on its target location in the TCMP and provides open issues and challenges, which has not been discussed in the previous works. The purpose of this survey

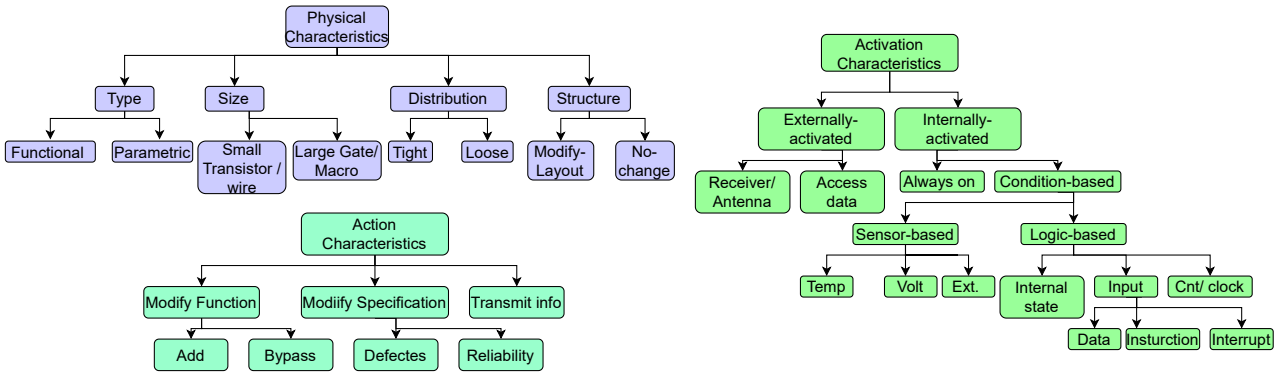

Fig. 2: Taxonomy of Trojans based on Physical, Activation, and Action characteristics

is to help the designers to better understand the skills of attackers, the amount of risk at each TCMP component, and the vulnerabilities that are exploited so that those factors are taken into consideration during the IC design and test cycle.

This paper investigates the impact of HT attack models in the TCMP. The rest of this paper is organised as follows: Section 2 presents the common security attacks that are needed for design consideration in hardware security methods. Section 3 presents the most recent HT attacks in the TCMP platform. Section 4 presents a comprehensive review of available mitigation methods for the current HT attacks. Section 5 demonstrates the open issues and challenges based on these available attack models, followed by the conclusion in Section 6.

II. Attack Model and Mitigations

In order to safeguard the entire hardware system against hostile interference, it is imperative that we are aware of the security flaws in contemporary intelligent gadgets. Basic hardware attack types, potential issues, and HT categorization according to TCMP are covered in this section.

A. Hardware Trojans

HT refers to the unethical modification of circuitry to extract sensitive information. HT insertion can be performed in two ways. The first way is modifying or altering the lithographic masks, specifically when an adversary inserts a Trojan in the design by adding, removing, or changing logic gates [31]. The second way is insertion of HT during fabrication phase or simply ignoring any HT that is detected during the testing phase. HT insertion can be also possible by 3PIP.

It can be categorized according to their physical, activation, and action characteristics as shown in Figure 2. There are always on and rarely activated Trojans from which some are implemented digitally, and others are analogically [31]. In similar fashion, there are also two types of HT detection techniques: destructive and non-destructive [32]. The destructive approaches are extremely expensive and as an adversary might affect only a small population of the manufactured ICs, destructive reverse engineering approaches cannot be effective for trust validation in ICs.

The non-destructive approaches can be classified in two ways: non-invasive and invasive. The invasive detection methods alter the layout to incorporate elements meant to identify Trojans whereas the non-invasive detection methods depend on external parametric and functional IC testing, such as observing input and output patterns, delay, and power leakage.

The HT circuit requires trigger condition, trigger signal, and payload. If the trigger condition matches with the HT condition, then the trigger signal gets activated which propagates the malicious payload from the original circuitry.

System-on-chip (SoC) integration or IC fabrication outsources IPs from 3PIP due to lower manufacturing costs, design complexity, and time-to-market pressure. These IPs include physical layout IP (hard IP), gate-level netlist IP (firm IP) and register transfer-level IP (soft IP) [32]. The involvement of 3PIP leads to IP security issues that include IP cloning, IP imitation, and the Trojan insertion scenarios.

In a similar fashion, an adversary can work within the foundry and modify the soft IP or pirate the 3PIP for malicious intentions like leaking private key or destroying a system.

B. Challenges

A diverse supply chain for integrated circuits is also necessary due to the increasing complexity of IC design. The IC supply chain is involving more and more individuals and nations, which expands the potential for hardware attacks. One of the common challenges for IoT devices is to provide security with low energy capacity. In general, when the security primitives are upgraded the energy consumption will increase proportionally. This leads to trade-offs between security, power consumption, and performance [43]. Additionally, after the designing stage, it is very expensive and difficult to identify hardware level flaws. Therefore, appropriate test in an early stage of design is essential to reduce malfunctions in the IC.

III. HT Attack Models in TCMPs

In this section, we elaborately discuss about the current attack models on the TCMP platform. For example, M3 platform [3] and PULP platform [44] are existing commercially available TCMP products. The internal architecture of the tile, router, network interface, and the possible attack models for each location are shown in Figure 3.

Generally, a tile in TCMP consists of a Processor, an L1 Cache, an L2 Cache, a Network Interface (NI), and a Cache Controller (CC). The L2 cache is shared and the L1 cache is private. The NoC router comprises Input Port Buffers, Routing

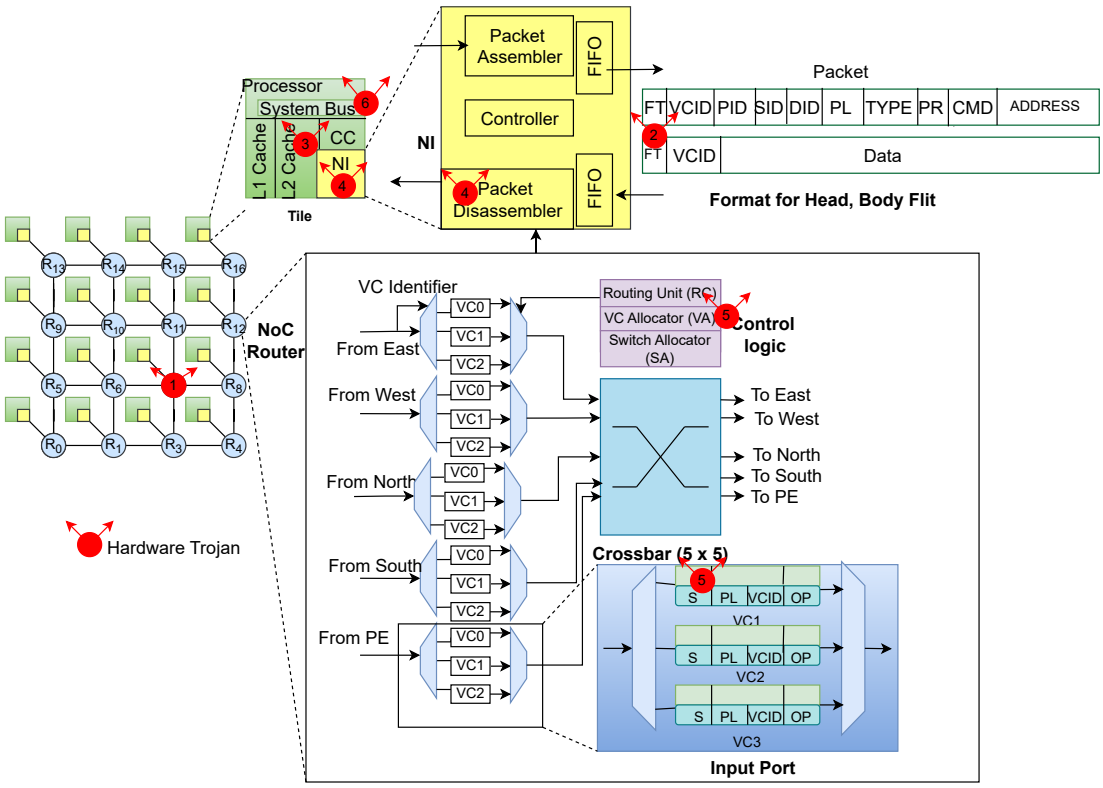

Fig. 3: Possible HT attack model in different places in Tiled Chip Multi-Core Processor systems

Unit, Virtual Channel Allocator (VA), Switch Allocator (SA), and a Crossbar. Figure 3 shows the input port of a router with three Virutal Channels (VCs). A maximum of three flits can be accommodated at a time by each VC, which is a FIFO. Separately, each VC keeps a control buffer comprising Output Port (OP), Virtual Channel Identifier (VCID), Status (S), and Packet Length (PL). When a flit arrives at a router, the input port demultiplexer inserts the flit into the specified VC after removing the VCID from the incoming flit's common prefix. If it is a head flit, the PL field of the flit is copied to the PL of the control buffer, and S is set to busy. In order to determine the next outgoing port, the routing unit takes Destination ID from the head flit and updates OP accordingly. Hence, once the routing is done for a head flit, then OP holds the next outgoing port information for all the subsequent flits of that packet. The OP field get reset when the tail flit leaves the router. For every head flit, the VC Allocator allocates a new VC based on the VC availability at the next downstream router.

In TCMP, the communication between source and destination tiles is packet-based, data travels in the form of flits between a pair of adjacent routers. The packet consists of header, body, and tail flits. The header contains routing information that directs the packet to the intended destination. The flit format is shown in Figure 3 where FT specifies the flit type, VCID is the virtual channel ID. The VCID specifies which location it holds after reaching the next router. PID works as a unique identifier for packets within the network. The SID and DID works as the IDs of the source and destination tiles respectively. PL denotes the number of non-head flits in a given packet. The TYPE field specifies the packet type. A priority is assigned to each packet in the PR field. The CMD field is used for storing additional metadata about the packet. The Address field denotes the physical address that needs to communicated between memory levels [45].

An HT can be inserted in a module of the TCMP such as in the router to disrupt message passing [42], [46]–[48], rerouting packets [49], [50], network interface to attack the packet [51] or to change or modify the head or body flit [52]–[54], cache coherence to leak confidential data [45], [55], [56], virtual channel allocator to capture the original flit and alter it with a malicious flit [57]–[59]. Table I depicts each of the works with the corresponding objective and the location where the attack model is introduced. A high-level overview of potential attack scenarios are shown in Figure 3. Suggestions for places that require careful design to mitigate these kinds of HTs are provided by summarizing HT attack models in Table I.

A. Attack Models by Malicious Routers

In this section, we will discuss the state-of-the-art(SotA) HT attack models in routers in TCMP. In Figure 3 HT symbol with mark 1 signifies the location of these attack models. In TCMP to communicate from one tile to another tile the NoC is mainly used. Packet-based NoC is a widely used solution for on-chip communication between IPs in complex SoCs. Router is a networking device in NoC which forwards data packets between computer networks. Hence, if the router is attacked then the data forwarding will be affected which leads to a compromised TCMP system.

Daoud et al. [42], [47] proposed a black hole router attack where a malicious router will silently drop the received packet. The malicious router will perform successful handshaking operation with the benign sender router and then drops the packet instead of sending it to the next router or the destination router. A similar kind of HT is presented in [48], where activating the HT causes misrouting of the packets to initiate a denial of service, delay of service, and injection suppression. The routing algorithm employed to decide the next router is HT infected. Due to the misrouting, the packet never reached the destination router. Also, the misrouting will cause huge delay in the arrival of packets to the desired destination.

Work in [51] exploits the on-chip temperature sensor information to identify the hotspot nodes and launch an attack on multicast packets to degrade the performance of the network-on-chip. This thermal packet is then intercepted by the HT which compares the node temperature with the temperature threshold to determine if the node is a hotspot. Every multicast packet passing through the infected router will be modified to add all identified hotspot nodes as a destination. The modified multicast packet will exacerbate the situation, finally degrade the performance of the network.

A blaming HT (BHT) [46] can cause a significant security risk for several HT mitigation strategies. BHT blames other innocent routers as HT in the network. A dynamic shield is built around these routers in accordance with SECTAR [48]. In this scenario, the traffic bypasses these false HT routers via the shielding routers. This results in less number of routers working in the NoC, affecting the system performance. There can be multiple consequences of BHT routers such as generating multiple false HT routers in the NoC, taking unnecessary long paths, increasing network congestion, causing injection suppression problems in workload with high miss per thousand instructions (MPKI), and can make a segment of TCMP unreachable by isolating the victim router from other NoC which in turn isolate the application running in the local tile from others.

Sankar et al. [49] introduced an attack model where a router and a processor in a tile are HT infected. The HT, which is in the XY path between any two routers duplicates copies of packets passing through it and sends them to the router that is connected with malicious tile. The HT in the malicious tile can use the header information and raw payload for malicious activities. Bagga et al. [50] presents an HT whose main objective is misrouting and creating huge amount of delay in packet transfer approach. According to the attack model, during a packet transfer from a source router to a destination router, the HT router will retransfer the packet to the source router. The packet will oscillate and after a certain period, it will reach to destination port due to the intermittent HT.

B. Attack Models in Packets

The router communicates with another router in a TCMP system by transferring packets. As introduced in the beginning of this section the packet consists of header, body, and tail flits. In this section, we will discuss the attack models in packets which is shown in Figure 3 by HT marked with 2.

Jyv et al. [52] proposed an HT attack which is triggered by a particular complex bit pattern from input messages and tries to mislead the packets away from the destined addresses. The flit, after entering the router through one of its input ports gets stored in the buffer queue. When the designed trigger condition is met on the input flit, the payload mechanism changes the particular field and then stored in the buffer. The modified flit then passes to the crossbar switch and with the help of route computation module, it gets forwarded to another node. It starts affecting different components of router based on the field effected. The Trojans used for the work are Flit Quantity Trojan (QT), Address Trojan (AT), and Head Hardware Trojan (HHT) and Tail Hardware Trojan (THT). The mentioned Trojans target the quantity of the flit causing a performance decline.

Similarly, when additional dummy flits are inserted then it cause performance degradation. A novel HT [59] is modeled that alters the common prefix field of NoC packets which leads to dead flits in router buffers. The described HT is always active, however an attack is triggered randomly with a probability p. When a flit enters the infected router, the proposed HT modifies the Flit Type(FT) field before routing and Virtual Channel (VC) allocation operations are carried out. Two variants of this proposed HT is introduced where one HT modifies the head flit to body flit (HT-HB) and another one modifies the body flit to head flit (HT-BH). Since every packet has a head flit, HT-HB can act on any packet passing through the infected router, however, HT-BH can impact only packets with body flits, mostly cache miss reply and write back packets. This type of HT can impact the core, cache, and NoC level.

An HT model presented in [53] proposed that an HT is mounted on the input buffers of NoC routers that can alter the destination address field of selected NoC packets. The HT can completely halt an application stalling instruction and can significantly impact the miss penalty of L1 caches. The HT manipulates the head flit when it is residing in the VC of the HT infected router. Once the Output Port (OP) and Virtual Channel Identifier (VCID) is computed and updated by route computation and VC allocator, respectively, the HT modifies destination ID field of the L1-cache miss request packets. The new destination ID can still be reached by underlying XY routing technique without any turn violations. The L1 miss request packet is chosen for HT attack because L1 miss penalty impacts processor throughput to a larger extent.

Authors in [45] proposed a Delay Trojan (DT) that can attack packets when they reside in the input port buffer of the infected router. The DT facilitates this by blocking the control signals that trigger the route computation activity, which disables the routing operation. After a random number of delay cycles, the control signal is activated again, causing the delayed packet to be routed and arbitrated, and the packet to be sent to its destination. The DT increases the miss penalty of critical L1 cache misses by creating a congestion in the path of a few random cache miss request packets.

TABLE I: Attack Models in different parts of TCMPs

Categories of Attack Model Based on Location	**Objective**	**Work**
Router	Black Hole Router Attack	[42], [47]
	Misrouting of Packets	[48]
	Identification of hotspot by temperature sensor to attack multicast packets	[51]
	Blaming Hardware Trojan Router indicates innocent router as HT router	[46]
	Packet duplication and transfer router with complicit application	[49]
	Intentionally altering the destination router to cause Delay	[50]
Packet	Attack on Flits	[52]
	Dead Flit Attack	[59]
	Packet Header Attack	[53]
	Delay Trojan that increases the miss penalty of critical L1 cache misses	[45]
Cache Coherence	Injects malicious memory transactions onto the main interconnect	[60]
	Intercepting coherence messages from the network interface	[56], [61]
Network Interface	Duplicate flit in the flit queue to increase the latency	[57]
	HT attack on Last Level Cache resizing	[55]
Virtual Channel Allocator	Duplicates incoming packets	[62]
	Altering state of the virtual channel. Causing delay in the arrival of the packets	[58]
System Bus	Covertly sniffing the interconnect bus	[54]

C. Attack Models in Cache Coherence

Cache coherency is a situation where multiple processor cores share the same memory hierarchy, but have their own L1 data and instruction caches. In this section we will discuss about HTs that are designed to attack cache coherence. In Figure 3 the location is marked with HT symbol 3.

The CPUs or hardware accelerators interfaced with the system bus or NoCs are the target places for the HT insertion [60]. The injected traffic forces the eviction of cache lines, taking advantage of cache coherence protocols. This type of Trojans insidiously slows down the system performance. Two Trojan models are designed to fulfil the malicious purpose of the attacker. The first Trojan model exploits the back-invalidation property of an inclusive cache to slow down the system performance while the second Trojan model injects the write invalidation transactions to the main interconnect. While a malicious write transaction (not invalidation) changes the system state and most likely results in the system crash, the write invalidation transaction causes the caches to simply invalidate the corresponding cache line. These kinds of attacks are insidious as the invalidation write transactions do not alter the system state and simply slows down the performance.

A complex Trojan attack in a chiplet-based system is demonstrated in [56], [61]. A Forging Attack that manipulates legal coherence transactions to allow a Trojan to write to a target address in a different process operating in a different chiplet. The compromised chiplet containing the Trojan does not have access to the victim process' address space but can observe broadcasted coherence interactions. The chiplet systems will rely heavily on coherence to ensure that data remains up-to-date in all components, making the coherence protocol an attractive target. The Trojan is complex and it modifies memory without relying on malicious software.

D. Attack Models in Network Interface

The network interface generates packets based on the message type (Request, Reply, or Coherence), which are forwarded to the appropriate router associated with it. The HT symbol marked with 4 in Figure 3 presents the location of HT.

Authors in [57] proposed an HT which is mounted in the Network Interface (NI) of a malicious IP and can be triggered by specific inputs. LOKI [57] selectively duplicates NoC control packets to attack SoC components. It is shown that when the attacker triggers LOKI, packet latency, miss penalty and system speedup are severely affected thereby degrading the overall SoC performance. It continuously keep inserting the duplicate flit into the Flit Queue until the kill switch is disabled. The duplicated flits are inserted in the free locations to avoid interrupting the usual flow of inter IP communication.

Kumar et al. [55] targets the Last Level Cache (LLC) resizing techniques. The LLC resizing techniques are used to reduce the energy consumption of the LLC by shutting down unused parts of the LLC. The proposed attack can misuse the properties of these resizing techniques to reduce their energy saving up to 58% and can also reduce the system performance up to 18%. To fulfill the objective three variants of HT attack are explored in this work. The first two attacks assume that the HT is present at the network interface (NI) of the tile hosting the resizing manager (RM). For the first attack (Random Attack), the NI supplies incorrect information related to the banks to the RM. Based on this information the RM takes wrong decision in LLC resizing. The second (Targeted RM Attack) and third attacks (Targeted Bank Attack) target a particular bank for forceful shutdown or restart, ignoring the advice of RM. The third attack assumes that the HT can be present at the NI of any tile. The attack drastically reduces the energy saving achievable by the LLC resizing techniques.

E. Attack Models in Virtual Channel Allocator

The VC allocator allocates every head flit in a VC based on the availability. This section provides the attack models in VC allocator which is displayed in Figure 3 by HT symbol marked with 5. Ancajas et al. [62] specifies an attack model in a 4-stage virtual-channel (VC) router pipeline. The four stages are the input buffers/route calculation, VC allocation, switch allocation and switch traversal. An HT that duplicates incoming packets from the local processing element can be inserted in each or one of the ports. The trojan taps the incoming links from the network interface (NI) and watches out for covert signals from a possible accomplice thread.

A novel HT is proposed in [58] that can attack the network resources by altering the status of the Virtual Channel (VC). It results in delaying the processing of packets to their destination tile. The HT is localized in the input buffer of the Virtual

TABLE II: Countermeasures and mitigation approaches for the attack models

Location	Attack Model	Countermeasure & Mitigation Approach
Router	multicast packets [51]	multicast routing [51]
	misrouting of packets [53]	dynamic shielding [48], [53]
	packet duplication [49]	SecNoc [49]
	HT in NoC [37]	PortBlocker [50]
	HT in NoC	Evolutionary Algoritm [63]
	compromised NoC [64]	Fort-NoCs [64], [65], [66]
Packets	attack on flits [52]	bit shuffling
	delay trojan [45]	dynamic adaptive caging [45]
System Bus	attack in Bus	secure bus architecture [67], [68]
Whole TCMP System	attack in any possible areas in TCMP	Trustworthy design [3], PMPGuard [69], DCI & DSCT [70]

Channel. The disruption caused by HT creates a small delay, the packet tends to reach its destination later than normal.

F. Attack Models in System Bus

A system bus is a single computer bus that connects the major components of a computer system, combining the functions of a data bus to carry information, an address bus to determine where it should be sent or read from, and a control bus to determine its operation. In Figure 3 HT symbol 6 shows the location of the attack model.

An HT in [54] can secretly sniff the interconnect bus to detect encrypted data streams. The HT, hidden in the system bus (wishbone interconnect), intelligently detects and identifies the specific IP core which sends an encrypted data stream to the processor. After detecting an encrypted data stream, the HT identifies the address of the originating peripheral from the bus communication packets.

IV. Countermeasures Against HTs in TCMP

This section describes the possible countermeasures that can detect some of the mentioned HT models mentioned in Section III. As the attack models are different based on their implementation location and design techniques, there is no single mitigation or detection approach available in the market that can solely detect all the attack models. Table II gives an overview of the possible countermeasures and mitigation techniques depending on the discussed attacks in Table I.

The countermeasures that are focused on attack models in routers are noted in second row of Table II and are differentiated based on individual attack models. For example, authors in [51] presents a hierarchical multicast routing algorithm which combines multiple unicast and multipath routing, to avoid Trojan attack in routers. The work misrouting of packet [53] is mitigated by implementing dynamic shielding [53] approach. A novel kind of detection approach is done by [48] using dynamic shielding and secure routing algorithm. Work in [49] presented a lightweight authenticated encryption system called Sec_{NoC} for secure packet transmission to evade packet duplication. Also, [50] proposed a port block detection strategy to detect Trojans incorporated in the routers [37]. Authors in [63] proposes an evolutionary algorithm based method to mitigate HT attacks in NoC of Coarse-Grained Reconfigurable Arrays (CGRA). Similar kind of work is presented in [64] where Fort-NoCs is presented which demonstrate a series of technique that work together to provide protection from compromised NoC in an MPSoC. The work [65] proposes a method which uses flit integrity and dynamic flit permutation to eliminate HT inserted in the router of the NoC. Later, [66] modified the work presented in [65] for better improvement.

In the second row of the Table II the mitigation approaches for HT attacks on packets are specified. The work in [52] presents a bit shuffling method to mitigate the attack on flits. A dynamic adaptive caging detection procedure is presented in [45] to cope up with the delay trojan attack.

The detection procedure based on system bus related attacks are noted in third row of Table II. Works in [67], [68] present a system-on-chip bus architecture for protection from HT. In the last row of Table II, the mitigation or detection approaches that are focused on the whole TCMP system are considered. Work in [3] proposes an isolation based solution in the tiled architecture with the help of trusted communication unit (TCU) so that malicious event can not propagate from one tile to another and the system apart from the HT infected tile is still secure. Authors in [69] proposes a pipeline multi processor guard (PMPGuard) that detects the presence of HT in 3PIP cores of PMPSoCs. In [70], authors present an approach that allows detection and localization of HT, which is based on the use of packet information and machine learning algorithms.

Therefore, it can be outlined that most of the mitigation approaches are targeted on the attack models based on the NoC router. However, more generalized countermeasures are required to consider all the attack models focused on the other components in TCMPs such as NI, cache coherence, or VC allocator.

V. Open Issues and Challenges

We have observed the feasibility of HT attacks on different areas in TCMP starting from the NoC to the system bus. The works surveyed for HT attacks on TCMPs are mostly applicable at the design and synthesis phases compared to the fabrication and assembly phases. All the attack models [42], [47] based on routers or packets [53] target the performance degradation of the network as the HT payload function. Some attacks [60] are extremely harmful as they can slow down the system performance without changing the system state. Though all the components are prone to HT attacks, NoC and routers are the main focus of most of the attack models. This leads to a direction of mitigation techniques that are mostly focused on HT detection in the NoC area.

It is quite difficult to find a "silver bullet" solution that can consistently defend against all these current Trojan attacks of all shapes, sizes, and varieties. The proposed detection approaches are all attack model-specific, and none of them can exhaustively detect HTs. If each of the tiles and interconnects between the tiles are trusted by an additional component, then these attacks can be mitigated. Therefore, mitigation techniques that combine the usefulness of a Trojan-aware design with verified pre-silicon as well as post-silicon tests can be effective for secure and trustworthy applications. Future work would focus on major areas related to HTs: 1) investigating the latest attack models, especially, attacks in

unexplored areas of TCMP apart from NoCs and routers; 2) developing formally verified IPs and then for each translation step a formal proof can prevent any alteration which will nullify many attacks; 3) novel mitigation approaches. Future research on mitigation approaches would incorporate detection strategies for unknown attack models, that not only cover one specific area of a TCMP but also more areas can be covered with a single detection strategy.

VI. Conclusion

In this work, we surveyed the HT attack models that are implemented in the TCMP platform. These attacks pose a danger since they can use one or more attack surfaces, an implementation strategy, and stealthier HTs to avoid detection. An additional angle on an attack might involve an adversary gaining access to private information through an implanted HT in a user's system. There can be unlimited possibilities where HT insertion is possible but the approach is to build an SoC platform in such a way that it cannot be harmed by these hardware attacks. These attack models will help the research domain to reconfigure the vulnerable parts of the TCMP to maintain the security aspect.

VII. ACKNOWLEDGMENT

This research is funded by the European Union's Horizon Europe research and innovation program under grant agreement No. 101094218 (CYMEDSEC) and No. 101092598 (COREnext). It is also financed on the basis of the budget passed by the Saxon State Parliament in Germany.

References

[1] Oyekunle Ayinde Olukotun, Lance Hammond, and James P Laudon. *Chip multiprocessor architecture: techniques to improve throughput and latency*, volume 3. Morgan & Claypool Publishers, 2007.

[2] Luca Benini and Giovanni De Micheli. Networks on chips: A new soc paradigm. *computer*, 35(1):70–78, 2002.

[3] Friedrich Pauls, Sebastian Haas, Stefan Köpsell, Michael Roitzsch, Nils Asmussen, and Gerhard Fettweis. On trustworthy scalable hardware/software platform design. In *2022 Smart Systems Integration (SSI)*, pages 1–6, 2022.

[4] Nachiketh Potlapally. Hardware security in practice: Challenges and opportunities. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pages 93–98. IEEE, 2011.

[5] Sally Adee. The hunt for the kill switch. *IEEE Spectrum*, 45(5):34–39, 2008.

[6] Mohammad Tehranipoor and Farinaz Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE design & test of computers*, 27(1):10–25, 2010.

[7] Yier Jin, Nathan Kupp, and Yiorgos Makris. Experiences in hardware trojan design and implementation. In *2009 IEEE international workshop on hardware-oriented security and trust*, pages 50–57. IEEE, 2009.

[8] Ramesh Karri, Jeyavijayan Rajendran, Kurt Rosenfeld, and Mohammad Tehranipoor. Trustworthy hardware: Identifying and classifying hardware trojans. *Computer*, 43(10):39–46, 2010.

[9] Alex Baumgarten, Michael Steffen, Matthew Clausman, and Joseph Zambreno. A case study in hardware trojan design and implementation. *International Journal of Information Security*, 10:1–14, 2011.

[10] Takeshi Kumaki, Masaya Yoshikawa, and Takeshi Fujino. Cipher-destroying and secret-key-emitting hardware trojan against aes core. In *2013 IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 408–411. IEEE, 2013.

[11] Rana Elnaggar, Krishnendu Chakrabarty, and Mehdi B Tahoori. Hardware trojan detection using changepoint-based anomaly detection techniques. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(12):2706–2719, 2019.

[12] M Meraj Ahmed, Abhijitt Dhavlle, Naseef Mansoor, Purab Sutradhar, Sai Manoj Pudukotai Dinakarrao, Kanad Basu, and Amlan Ganguly. Defense against on-chip trojans enabling traffic analysis attacks. In *2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pages 1–6. IEEE, 2020.

[13] Abhishek Vashist, Andrew Keats, Sai Manoj Pudukotai Dinakarrao, and Amlan Ganguly. Securing a wireless network-on-chip against jamming based denial-of-service attacks. In *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 320–325. IEEE, 2019.

[14] Ferdinand Brasser, Lucas Davi, Abhijitt Dhavlle, Tommaso Frassetto, Sai Manoj Pudukotai Dinakarrao, Setareh Rafatirad, Ahmad-Reza Sadeghi, Avesta Sasan, Hossein Sayadi, Shaza Zeitouni, et al. Advances and throwbacks in hardware-assisted security: Special session. In *Proceedings of the International Conference on Compilers, Architecture and Synthesis for Embedded Systems*, pages 1–10, 2018.

[15] Kanad Basu, Samah Mohamed Saeed, Christian Pilato, Mohammed Ashraf, Mohammed Thari Nabeel, Krishnendu Chakrabarty, and Ramesh Karri. Cad-base: An attack vector into the electronics supply chain. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 24(4):1–30, 2019.

[16] Christian Pilato, Kanad Basu, Francesco Regazzoni, and Ramesh Karri. Black-hat high-level synthesis: Myth or reality? *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(4):913–926, 2018.

[17] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, Xuan Thuy Ngo, and Laurent Sauvage. Hardware trojan horses in cryptographic ip cores. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 15–29. IEEE, 2013.

[18] Samaneh Ghandali, Georg T Becker, Daniel Holcomb, and Christof Paar. A design methodology for stealthy parametric trojans and its application to bug attacks. In *Cryptographic Hardware and Embedded Systems–CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings 18*, pages 625–647. Springer, 2016.

[19] Shugo Kaji, Masahiro Kinugawa, Daisuke Fujimoto, and Yu-ichi Hayashi. Data injection attack against electronic devices with locally weakened immunity using a hardware trojan. *IEEE Transactions on Electromagnetic Compatibility*, 61(4):1115–1121, 2018.

[20] Raghavan Kumar, Philipp Jovanovic, Wayne Burleson, and Ilia Polian. Parametric trojans for fault-injection attacks on cryptographic hardware. In *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 18–28. IEEE, 2014.

[21] MMeraj Ahmed, Abhishek Vashist, Sai Manoj Pudukotai Dinakarrao, and Amlan Ganguly. Architecting a secure wireless interconnect for multichip communication: An ml approach. In *2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, pages 1–6. IEEE, 2020.

[22] Mingfu Xue, Rongzhen Bian, Weiqiang Liu, and Jian Wang. Defeating untrustworthy testing parties: A novel hybrid clustering ensemble based golden models-free hardware trojan detection method. *IEEE Access*, 7:5124–5140, 2018.

[23] Muhammad Yasin, Ozgur Sinanoglu, and Jeyavijayan Rajendran. Testing the trustworthiness of ic testing: An oracle-less attack on ic camouflaging. *IEEE Transactions on Information Forensics and Security*, 12(11):2668–2682, 2017.

[24] Jean Kumagai. Chip detectives [reverse engineering]. *IEEE Spectrum*, 37(11):43–48, 2000.

[25] Matthew Smith Anderson, CJG North, and Kenneth K Yiu. Towards countering the rise of the silicon trojan. Technical report, 2008.

[26] Task Force. High performance microchip supply. *Annual Report. Defense Technical Information Center (DTIC), USA*, 2005.

[27] Swarup Bhunia, Michael S Hsiao, Mainak Banga, and Seetharam Narasimhan. Hardware trojan attacks: Threat analysis and countermeasures. *Proceedings of the IEEE*, 102(8):1229–1247, 2014.

[28] Robert Johnson. 'the navy bought fake chinese microchips that could have disarmed us missiles. *Business Insider*, 2011.

[29] Sergei Skorobogatov and Christopher Woods. Breakthrough silicon scanning discovers backdoor in military chip. In *Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14*, pages 23–40. Springer, 2012.

[30] Yousra Alkabani and Farinaz Koushanfar. Consistency-based characterization for ic trojan detection. In *Proceedings of the 2009 international conference on computer-aided design*, pages 123–127, 2009.

[31] Xiaoxiao Wang, Mohammad Tehranipoor, and Jim Plusquellic. Detecting malicious inclusions in secure hardware: Challenges and solutions.

In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 15–19. IEEE, 2008.

[32] Rajat Subhra Chakraborty, Seetharam Narasimhan, and Swarup Bhunia. Hardware trojan: Threats and emerging solutions. In *2009 IEEE International high level design validation and test workshop*, pages 166–171. IEEE, 2009.

[33] Kan Xiao, Domenic Forte, Yier Jin, Ramesh Karri, Swarup Bhunia, and Mohammad Tehranipoor. Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 22(1):1–23, 2016.

[34] Mingfu Xue, Chongyan Gu, Weiqiang Liu, Shichao Yu, and Máire O'Neill. Ten years of hardware trojans: a survey from the attacker's perspective. *IET Computers & Digital Techniques*, 14(6):231–246, 2020.

[35] Billel Guechi and Mohammed Redjimi. Hardware trojan detection in heterogeneous systems on chip. In *The Proceedings of the Third International Conference on Smart City Applications*, pages 1105–1116. Springer, 2020.

[36] Rajesh JS, Koushik Chakraborty, and Sanghamitra Roy. Hardware trojan attacks in soc and noc. *The Hardware Trojan War: Attacks, Myths, and Defenses*, pages 55–74, 2018.

[37] Sachin Bagga, Ruchika Gupta, and John Jose. Modelling and analysis of confluence attack by hardware trojan in noc. In *Emerging Electronic Devices, Circuits and Systems: Select Proceedings of EEDCS Workshop Held in Conjunction with ISDCS 2022*, pages 231–246. Springer, 2023.

[38] Lashmi Kondoth, Rajan Shankaran, Quan Z Sheng, and Richard Han. Wireless network-on-chip security review: Attack taxonomy, implications, and countermeasures. *IEEE Access*, 2023.

[39] Vivek Venugopalan and Cameron D Patterson. Surveying the hardware trojan threat landscape for the internet-of-things. *Journal of Hardware and Systems Security*, 2(2):131–141, 2018.

[40] Sonia Akter, Kasem Khalil, and Magdy Bayoumi. Hardware security in the internet of things: A survey. In *2023 IEEE 36th International System-on-Chip Conference (SOCC)*, pages 1–6. IEEE, 2023.

[41] Abhijitt Dhavlle, Rakibul Hassan, Manideep Mittapalli, and Sai Manoj Pudukotai Dinakarrao. Design of hardware trojans and its impact on cps systems: A comprehensive survey. In *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5. IEEE, 2021.

[42] Luka Daoud. Secure network-on-chip architectures for mpsoc: Overview and challenges. In *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 542–543. IEEE, 2018.

[43] Samuel Ellicott, Michael Kines, Waleed Khalil, Yu Qi, Abdullah Kurtoglu, and Hossein Miri Lavasani. Analog-inspired hardware security: A low-energy solution for iot trusted communications. In *2021 IEEE 34th International System-on-Chip Conference (SOCC)*, pages 200–205, 2021.

[44] Davide Rossi, Francesco Conti, Andrea Marongiu, Antonio Pullini, Igor Loi, Michael Gautschi, Giuseppe Tagliavini, Alessandro Capotondi, Philippe Flatresse, and Luca Benini. Pulp: A parallel ultra low power platform for next generation iot applications. In *2015 IEEE Hot Chips 27 Symposium (HCS)*, pages 1–39, 2015.

[45] Ruchika Gupta, Vedika J Kulkarni, John Jose, and Sukumar Nandi. Securing on-chip interconnect against delay trojan using dynamic adaptive caging. In *Proceedings of the Great Lakes Symposium on VLSI 2022*, pages 411–416, 2022.

[46] Bharat Bisht and Shirshendu Das. Bht-noc: Blaming hardware trojans in noc routers. 2022.

[47] Luka Daoud and Nader Rafla. Analysis of black hole router attack in network-on-chip. In *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 69–72. IEEE, 2019.

[48] R Manju, Abhijit Das, John Jose, and Prabhat Mishra. Sectar: Secure noc using trojan aware routing. In *2020 14th IEEE/ACM International Symposium on Networks-on-Chip (NOCS)*, pages 1–8. IEEE, 2020.

[49] Syam Sankar, Ruchika Gupta, John Jose, and Sukumar Nandi. Sec-noc: A lightweight secure communication system for on-chip interconnects. *IEEE Embedded Systems Letters*, 2023.

[50] Sachin Bagga, Ruchika Gupta, and John Jose. Portblocker: Detection and mitigation of hardware trojan through re-routing and bypassing. In *2023 IEEE 16th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC)*, pages 325–331. IEEE, 2023.

[51] Binayak Tiwari, Mei Yang, Yingtao Jiang, and Xiaohang Wang. Effect of hardware trojan attacks on the performance of on-chip multicast routing algorithms. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0623–0629. IEEE, 2019.

[52] Manoj Kumar JYV, Ayas Kanta Swain, Sudeendra Kumar, Sauvagya Ranjan Sahoo, and Kamalakanta Mahapatra. Run time mitigation of performance degradation hardware trojan attacks in network on chip. In *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 738–743. IEEE, 2018.

[53] Vedika J Kulkarni, R Manju, Ruchika Gupta, John Jose, and Sukumar Nandi. Packet header attack by hardware trojan in noc based tcmp and its impact analysis. In *Proceedings of the 15th IEEE/ACM International Symposium on Networks-on-Chip*, pages 21–28, 2021.

[54] Ali Murtaza, M Adeel Pasha, Shahid Masud, M Yasir Qadri, and Abdul Basit. Fpga based intelligent hardware trojan design and its soc implementation. In *2023 30th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, pages 1–4. IEEE, 2023.

[55] Atul Kumar, Shirshendu Das, and Basant Subba. Htree: Hardware trojan attack on cache resizing policies. *IEEE Embedded Systems Letters*, 2023.

[56] Gino A Chacon, Charles Williams, Johann Knechtel, Ozgur Sinanoglu, and Paul V Gratz. Hardware trojan threats to cache coherence in modern 2.5 d chiplet systems. *IEEE Computer Architecture Letters*, 21(2):133–136, 2022.

[57] Manju Rajan, Abhijit Das, and John Jose. Loki: a hardware trojan affecting multiple components of an soc. In *2022 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 176–181. IEEE, 2022.

[58] Abhishek Rana and Amandeep Kaur Sohal. Virtual channel attack by hardware trojan in noc-based tcmp and its impact analysis. In *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pages 507–511. IEEE, 2023.

[59] Mohammad Humam Khan, Ruchika Gupta, John Jose, and Sukumar Nandi. Dead flit attack on noc by hardware trojan and its impact analysis. In *Proceedings of the 14th international workshop on network on chip architectures*, pages 10–15, 2021.

[60] Minsu Kim, Sunhee Kong, Boeui Hong, Lei Xu, Weidong Shi, and Taeweon Suh. Evaluating coherence-exploiting hardware trojan. In *Design, Automation & Test in Europe Conference and Exhibition (DATE), 2017*, pages 157–162, 2017.

[61] Gino A Chacon, Charles Williams, Johann Knechtel, Ozgur Sinanoglu, Paul V Gratz, and Vassos Soteriou. Coherence attacks and countermeasures in interposer-based chiplet systems. *ACM Transactions on Architecture and Code Optimization*, 21(2):1–25, 2024.

[62] Dean Michael Ancajas, Koushik Chakraborty, and Sanghamitra Roy. Fort-nocs: Mitigating the threat of a compromised noc. DAC '14, page 1–6, New York, NY, USA, 2014. Association for Computing Machinery.

[63] Zeyu Li, Junjie Wang, Zhao Huang, and Quang Wang. Ea-based mitigation of hardware trojan attacks in noc of coarse-grained reconfigurable arrays. In *2022 International Conference on Networking and Network Applications (NaNA)*, pages 528–533, 2022.

[64] Dean Michael Ancajas, Koushik Chakraborty, and Sanghamitra Roy. Fort-nocs: Mitigating the threat of a compromised noc. In *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6, 2014.

[65] Jonathan Frey and Qiaoyan Yu. A hardened network-on-chip design using runtime hardware trojan mitigation methods. *Integration*, 56:15–31, 2017.

[66] Musharraf Hussain, Naveed Khan Baloach, Gauhar Ali, Mohammed ElAffendi, Imed Ben Dhaou, Syed Sajid Ullah, and Mueen Uddin. Hardware trojan mitigation technique in network-on-chip (noc). *Micromachines*, 14(4), 2023.

[67] Abhishek Basak, Swarup Bhunia, Thomas Tkacik, and Sandip Ray. Security assurance for system-on-chip designs with untrusted ips. *IEEE Transactions on Information Forensics and Security*, 12(7):1515–1528, 2017.

[68] Liu Changlong, Zhao Yiqiang, Shi Yafeng, and Gao Xingbo. A system-on-chip bus architecture for hardware trojan protection in security chips. In *2011 IEEE International Conference of Electron Devices and Solid-State Circuits*, pages 1–2, 2011.

[69] Amin Malekpour, Roshan Ragel, Tuo Li, Haris Javaid, Aleksandar Ignjatovic, and Sri Parameswaran. Hardware trojan mitigation in pipelined mpsocs. *ACM Trans. Des. Autom. Electron. Syst.*, 2020.

[70] Haoyu Wang and Basel Halak. Hardware trojan detection and high-precision localization in noc-based mpsoc using machine learning. In *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, pages 516–521, 2023.