Analysis of Black Hole Router Attack in Network-on-Chip

Luka Daoud, and Nader Rafla
Electrical and Computer Engineering
Boise State University, Boise, ID 83725
Email: LukaDaoud@u.boisestate.edu, nrafla@boisestate.edu

***Abstract*—Network-on-Chip (NoC) is the communication platform of the data among the processing cores in Multiprocessors System-on-Chip (MPSoC). NoC has become a target to security attacks and by outsourcing design, it can be infected with a malicious Hardware Trojan (HT) to degrades the system performance or leaves a back door for sensitive information leaking. In this paper, we proposed a HT model that applies a denial of service attack by deliberately discarding the data packets that are passing through the infected node creating a black hole in the NoC. It is known as Black Hole Router (BHR) attack. We studied the effect of the BHR attack on the NoC. The power and area overhead of the BHR are analyzed. We studied the effect of the locations of BHRs and their distribution in the network as well. The malicious nodes has very small area and power overhead, 1.98% and 0.74% respectively, with a very strong violent attack.**

***Keywords*—Blak Hole, BHR, Network-on-Chip, NoC, Hardware Trojan, HT, Denial-of-Service, DoS.**

I. Introduction

Due to advances in technology, billions of transistors can be crammed in an integrated circuit (IC) leading to embodying sophisticated systems in a single chip - known as System-on-Chip (SoC). SoC can include processing elements (PEs), storage segment, and other peripheral components along with networking unit. Network-on-Chip (NoC) architectures [1] have become the communication infrastructure of such computing elements, where hundreds of processing cores and memory modules are connected and communicating through the NoC. This enhances the system performance where applications are dynamically allocated on multiple PEs [2]–[4] and run simultaneously sharing the network resources.

NoC is the communication core of Multiprocessors System-on-Chip (MPSoC). In order to exchange information between PEs, messages are partitioned into packets and injected in the NoC. Therefore, transferring data via the NoC must be both reliable and secure. However, the semiconductor industry has started to flow a globalized business model for the integrated circuits (ICs) design flow. This has made the NoC vulnerable to security threats [5]–[7] by experiencing outsourcing design that may modify the original circuit design, known as Hardware Trojans (HTs), which potentially degrade system performance[8], surreptitiously delete data, or leave a backdoor for secret key leaking[7].

HTs can be embedded during any stage of the IC design flow or manufacturing phase [5] resulting from untrusted third party. Detection process of HT requires immense efforts and time. Additionally, it may still fail observation since HTs are designed in a way such that it is too difficult to be revealed. For large systems, such as networks on chip, it would be very hard and impractical to completely cover the whole system at test time. HTs have been able to bypass robust post-silicon tests due to their nature of being small enough to consume negligible amount of power compared to the whole system and/or being activated under very specific conditions to avoid disclosure.

Since NoC is the central communication platform among the PEs in the chip, it has become a target for security breach and degradation in the network performance. Most of NoCs have been developed without compromising security issues in the design. So far, most of the proposed solutions try to secure the cores and not the intercommunication itself inside the MPSoC. The NoC can be infected with HTs that are deployed in the routing nodes, known as malicious router (node). Unlike faulty nodes, where they are inoperative nodes and can be detected through post-silicon tests, malicious nodes interact with the system and silently apply their payload. The malicious circuits in the NoC are designed to attack the system in a variety of forms such as Denial of Service (DoS) attacks and system degradation [7]. In order for the system to notice security threats, a monitoring subsystem is embedded to observe inadequate behavior of the system, which are expensive and not scalable with the system. The research objectives and challenges are how to detect such malicious routers in runtime and efficiently avoid them.

In this paper, we proposed a HT model infecting a node(s) of the NoC to apply a denial of service attack by sinking all the packets, which are passing through them, and deliberately drops them. This infected node is known as black hole router (BHR). We performed an analysis of the BHR attack considering the area and power overhead of the malicious mode. We also suggested run time detection and avoiding protocol for BHR attacks. The rest of this paper is organized as follows: Background and the related works are explored in Section II, a HT threat model is explained in Section III, the evaluation of the BHR attack is analyzed in Section IV. Finally, Section V concludes the paper and provides suggestions for future work.

II. HT-based Attack in NoC

Hardware Trojan (HT) is a modification of the circuitry of the ICs for the purpose of leaving a backdoor for security threats or denial of service attack. It can be embedded

978-1-7281-2788-0/19/$31.00 ©2019 IEEE

during any stage of the IC design flow and manufacturing process [5]. Several studies have considered the HT attacks on NoC. In this section, we present the related work of HT-based denial of service attack targeting NoC. In [9], authors addressed HT issues in NoC links, where they used error control coding approach to detect the infected links between nodes in the NoC. They proposed a reshuffling scheme to avoid such attacked links, however, their method is limited to two victim wires of the link. Authors in [10] used the state-obfuscation technique to detect and protect the system, at runtime, from embedded HT in the finite state machine of the network interface. In [11], authors proposed a runtime latency auditor to detect traffic abnormalities caused by HT that suppresses allocation requests and de-prioritizes arbiters within the router controller to apply bandwidth DoS attack. The key problem with their technique is that it uses delay to detect such DoS attack, which is difficult to distinguish between bandwidth attack and latency during normal operation. In [12], a link HT that performs packet inspection and faults injection to apply DoS attack was examined. The proposed HT model exploited the vulnerabilities created by the fault-tolerant methods. The HT injects faults to link data which triggers the Error Correction Code (ECC) to detect errors and requests packet-retransmission. This leads to network resources (link) starving creating deadlock. In order to mitigate the suggested attack, they proposed a heuristic-based fault detection model. In [13], authors studied the effect of sinkhole attacks in NoC but power analysis and detailed distribution of the HTs in the NoC was not provided. In [8], authors proposed a HT model that applies DoS attack by misrouting the packets to degrade the NoC performance causing deadlock and virtually link failure.

In the previous work, different threat models were investigated to apply DoS attacks. In this paper, we study a HT-based threat model that is based on an infected router in the NoC, which deliberately drops packets that are passing through it. This is called black hole router (BHR) attack. We study the effect of the locations of the BHRs and their distribution in the NoC.

III. Black Hole Router Threat Model

Black hole router is a malicious node in the NoC that deliberately discards packets without a notice to the communication system. Therefore, any incoming or outgoing packets to or from a BHR are silently disappeared from the NoC. BHR is classified as a malignant node [7] and in order to silently drops the received packets, it follows the communication handshaking successfully and then it swallows the packet as soon as it is handled. Figure 1 shows an example of a black hole router (R3). The handshaking (shown as doted lines) between R1 and R2 are done successfully and the packet is completely forwarded. Similarly, a packet is sent from R2 and handed over to R3 auspiciously. However, R3 silently drops the packet and does not send it to R4 without further notice. It seems to the source (S), R1, and R2 that the packet is being forwarded successfully and neither R4 nor the destination (D) is aware of that.

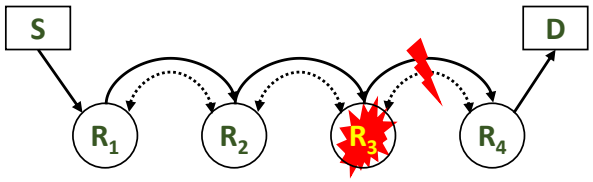


Fig. 1: An example of a black hole router

IV. Black Hole Router Attack Evaluation

A robust HT is the one that has unnoticeable footprint which makes it very difficult to detect. Additionally, the HT is designed to have three states which make them even harder to be disclosed during the offline test. The three states are *Inactive, Waiting, Attacking* and described in Table I.

TABLE I: States of the Hardware Trojan

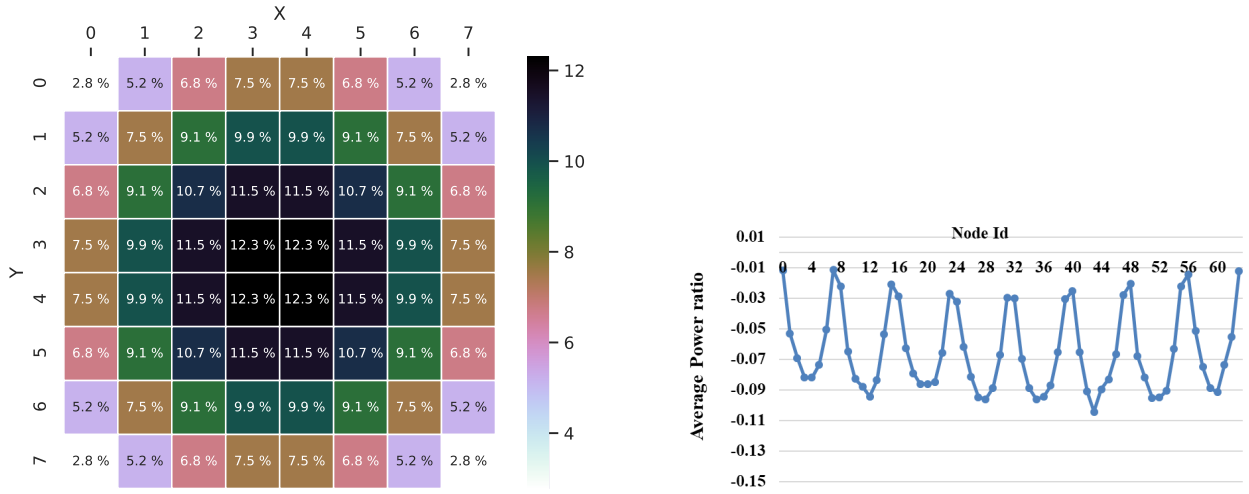
State	Description
Inactive	The Trojan is inactive and waiting for a trigger signal.
Waiting	The Trojan is ready and waiting to start its attack.
Attacking	The Trojan applies DoS attack in the NoC.

In order to evaluate the area and power overhead of a BHR, we designed a moderate size five-ports router with 8-flit depth FIFO in C/C++ language targeting high level synthesis (HLS)[14]. Vivado HLS [15] was used to generate the register transfer level (RTL) design. The design was synthesized using 45nm TSMC technology (Cadence Design Compiler) for area and power analysis. The baseline router has an area of 43180 μm^2 and power of 826.03 μW. We modified the base router and added the HT-based model along with the trigger circuit. The malicious router area and power overhead increased by 1.98% and 0.74%, respectively, of the baseline router which is too small to be revealed during the post-silicon test.

In order to evaluate the effect of the BHR attack in NoC, we developed a cycle accurate simulation environment in SystemC. Our baseline network is 8×8 Mesh NoC with X-Y routing technique. In particular, the simulations with different NoC sizes were performed and their analysis results are very similar to what is provided in this section. A number of factors are known to affect the BHR-based infected network, such as the number of the malicious nodes and their locations in the NoC, the traffic distribution of the packets, and the routing algorithm. In order to fairly analyze the affect of the BHRs locations and their distribution in the NoC, we set the spatial distribution of the traffic to a random uniform one. Table II shows the configuration parameters of the NoC.

TABLE II: NoC parameters

NoC parameter	**value**
NoC Size	8×8
input buffer depth	8
switching technique	Wormhole
routing algorithm	XY routing
traffic pattern	Uniform



(a) Packet loss percentage for each individual node

(b) Power consummation ratio during attack

Fig. 2: An 8×8 NoC under BHR attack

In the first experiment, we analyzed the effect of the location of the BHR in the NoC in terms of the number of the dropped packets and the consumed power. In this experiment, only one node of the NoC is infected with a BHR. The total number of dropped packets and the power consumption are measured. The simulation is repeated for another infected node and the outcome results are recorded. The simulation is repeated to cover each node in the NoC. Figure 2(a) shows the ratio of the packet loss to the total injected packets in the network. For example, when only node (3, 4) is infected with a malicious circuit, it drops 12.3% of the injected packets in the NoC. what can be clearly seen in this figure is that the packet-loss rate increases when the infected node is closer to the middle of the Mesh NoC. It is now clear that the location of the BHR in the NoC plays an important role in the attack. Figure 2(b) reveals the power consumption overhead with the infected nodes in the NoC. The graph shows that the infected NoC dissipates less power than the non-infected one. The reason behind this behaviour is the packet-discarding from the NoC via the BHR. As a result, the transmitter module in the infected router is not active and less packets are moving in the NoC. So, the more packet-loss rate is the less power dissipation.

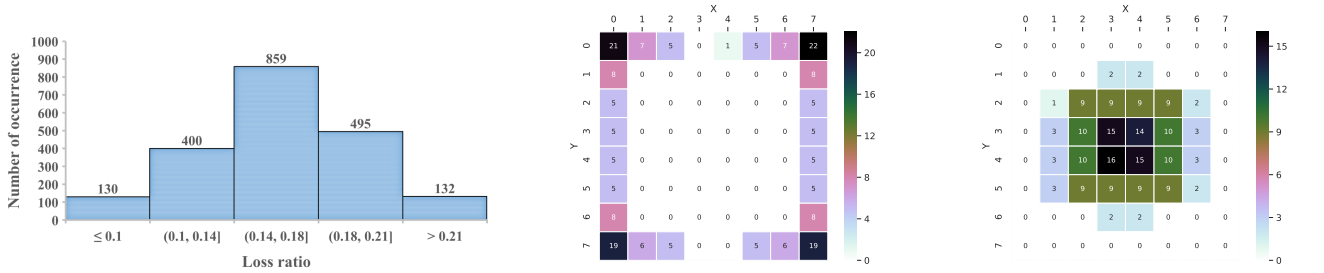
In the second experiment, the NoC is infected with two BHRs at a time. So, we have 2016, i.e. $\binom{64}{2}$, different distributions of two BHRs in the NoC. Figure 3 shows the analysis of a NoC attacked by two BHRs. The ratio of the dropped packets varies from 5.2% to 24.0% for all the combinations of the distribution of the two BHRs in the NoC. Figure 3(a) shows the frequency of loss rate periods. We notice that around half of the possible combinations of BHRs distribution has 14% to 18% of packet loss rate. Figure 3(b) and Figure 3(c) represents the distributions of two BHRs for the 100 minimum and maximum loss rate, respectively. The number in the box represents how many times this node was involved in the distribution the pair BHRs. It is obvious that the closer pairs to the center influences the maximum packet drop.

In the third experiment, we analyzed the effect of the average distance between the BHRs. In this demonstration, three BHRs infected the NoC. The packet loss rate and the average distance between the BHRs are captured. The average distance between three BHRs is measured as the average number of hops between each pair of them. Figure 4(a) shows the frequency of packet loss rate periods for the attacked NoC. The dropped packet rate varies from 7.4% up to 33.8% for all the combinations of the distribution of the three BHRs in the NoC and half of the possible combinations of BHRs distribution has 21% to 27% of packet loss rate. Figure 4(b) demonstrates the density of the packet loss rate along with the average distances between each possible three BHRs in the NoC. The graph reveals that when the average distance between the BHRs is medium (for example, the average distance = 6) , a higher density of packet loss rate is located at 21% to 27% category of the discarded packets.

Thus far, this section has reviewed the effect of the BHR in a NoC in terms of the location of the infected nodes, their number, and the average distance between them. Therefore, with less effort an attacker consider these factors to achieve a violent attack. On the other hand, this work shows the potency of a black hole router attacks a NoC. It is necessary to counteract a BHR attack. The countermeasure technique has two stages: first to detect such attacks, and second to avoid these malicious nodes. Once the BHR has been detected, a secure routing scheme [8] can be implemented to detour around the BHR and avoid their effect.

V. Conclusions and Future Work

In this paper, we presented a security threat model attacks the Network-on-Chip (NoC) through a Hardware Trojan. It is a packet dropping attack, where a malicious node in the NoC drops the packets that are passing through it. This is also known as a black hole router (BHR) attack. We studied the effect of the BHR on the NoC and analyzed the influence

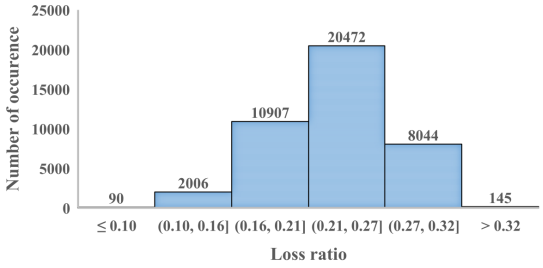


(a) Frequency of packet loss rate

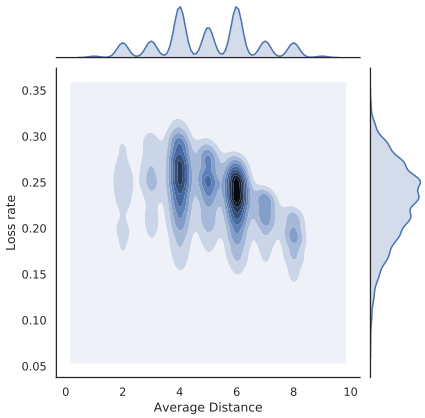
(b) Possibility distributions of two BHRs for minimum loss rate attack

(c) Possibility distributions of two BHRs for maximum loss rate attack

Fig. 3: An 8×8 NoC under two BHRs attack



(a) Frequency of the packet loss rate



(b) Density of the packet loss rate with the average distance between the BHRs

Fig. 4: An 8×8 NoC under three BHR attack

of the number of the BHRs along with their distribution in the NoC on the potency of the attack. The packet loss rate varies between 5% to 33.8% based on the number of BHRs and their locations in the NoC. Future work could include runtime detection of the BHR and a malicious-tolerant routing technique to avoid such infected nodes.

REFERENCES

[1] L. Benini and G. De Micheli, "Networks on chips: A new soc paradigm," *computer*, vol. 35, no. 1, pp. 70–78, 2002.

[2] L. B. Daoud, M. E.-S. Ragab, and V. Goulart, "Faster processor allocation algorithms for mesh-connected cmps," in *Digital System Design (DSD), 2011 14th Euromicro Conference on*, pp. 805–808, IEEE, 2011.

[3] L. B. Daoud, M. E.-S. Ragab, and V. Goulart, "Processor allocation algorithm based on frame combing with memorization for 2d mesh cmps," in *Circuits and Systems (LASCAS), 2012 IEEE Third Latin American Symposium on*, pp. 1–4, IEEE, 2012.

[4] L. Daoud and V. Goulart, "High performance bitwise or based submesh allocation for 2d mesh-connected cmps," in *Digital System Design (DSD), 2013 Euromicro Conference on*, pp. 73–77, IEEE, 2013.

[5] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware trojan design and implementation," in *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on*, pp. 50–57, IEEE, 2009.

[6] J.-P. Diguet, S. Evain, R. Vaslin, G. Gogniat, and E. Juin, "Noc-centric security of reconfigurable soc," in *Networks-on-Chip, 2007. NOCS 2007. First International Symposium on*, pp. 223–232, IEEE, 2007.

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

[8] L. Daoud and N. Rafla, "Routing aware and runtime detection for infected network-on-chip routers," in *IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 775–778, IEEE, Aug 2018.

[9] Q. Yu and J. Frey, "Exploiting error control approaches for hardware trojans on network-on-chip links," in *Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2013 IEEE International Symposium on*, pp. 266–271, IEEE, 2013.

[10] J. Frey and Q. Yu, "Exploiting state obfuscation to detect hardware trojans in noc network interfaces," in *Circuits and Systems (MWSCAS), 2015 IEEE 58th International Midwest Symposium on*, pp. 1–4, IEEE, 2015.

[11] R. JS, D. M. Ancajas, K. Chakraborty, and S. Roy, "Runtime detection of a bandwidth denial attack from a rogue network-on-chip," in *Proceedings of the 9th International Symposium on Networks-on-Chip*, p. 8, ACM, 2015.

[12] T. Boraten and A. Kodi, "Mitigation of hardware trojan based denial-of-service attack for secure nocs," *Journal of Parallel and Distributed Computing*, vol. 111, pp. 24–38, 2018.

[13] L. Zhang, X. Wang, Y. Jiang, M. Yang, T. Mak, and A. K. Singh, "Effectiveness of ht-assisted sinkhole and blackhole denial of service attacks targeting mesh networks-on-chip," *Journal of Systems Architecture*, vol. 89, pp. 84–94, 2018.

[14] L. Daoud, D. Zydek, and H. Selvaraj, "A survey of high level synthesis languages, tools, and compilers for reconfigurable high performance computing," in *Advances in Systems Science*, pp. 483–492, Springer, 2014.

[15] Xilinx Inc., *Vivado Design Suite User Guide: High-Level Synthesis*, December, 2018.