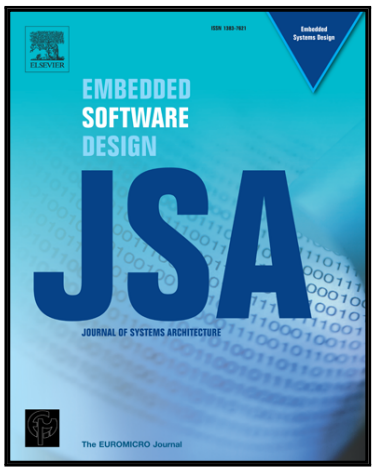


Effectiveness of HT-assisted Sinkhole and Blackhole Denial of Service Attacks Targeting Mesh Networks-on-chip

Li Zhang, Xiaohang Wang, Yingtao Jiang, Mei Yang, Terrence Mak, Amit Kumar Singh

PII: S1383-7621(18)30067-5
DOI: https://doi.org/10.1016/j.sysarc.2018.07.005
Reference: SYSARC 1512

To appear in: *Journal of Systems Architecture*

Received date: 5 March 2018
Revised date: 12 July 2018
Accepted date: 25 July 2018

Please cite this article as: Li Zhang, Xiaohang Wang, Yingtao Jiang, Mei Yang, Terrence Mak, Amit Kumar Singh, Effectiveness of HT-assisted Sinkhole and Blackhole Denial of Service Attacks Targeting Mesh Networks-on-chip, *Journal of Systems Architecture* (2018), doi: https://doi.org/10.1016/j.sysarc.2018.07.005

Effectiveness of HT-assisted Sinkhole and Blackhole Denial of Service Attacks Targeting Mesh Networks-on-chip☆

Li Zhang[a], Xiaohang Wang[a,*], Yingtao Jiang[b], Mei Yang[b], Terrence Mak[c], Amit Kumar Singh[d]

[a] *South China University of Technology, China*
[b] *University of Nevada, Las Vegas, USA*
[c] *University of Southampton, UK*
[d] *University of Essex, UK*

Abstract

There are ample opportunities at both design and manufacturing phases to meddle in a many-core chip system, especially its underlining communication fabric, known as the networks-on-chip (NoC), through the inclusion of malicious hardware Trojans (HT). In this paper, we focus on studying two specific HT-assisted Denial-of-Service (DoS) attacks, namely the sinkhole and blackhole attacks, that directly target the NoC of a many-core chip. As of the blackhole attacks, those intermediate routers with inserted HTs can stop forwarding data packets/flits towards the packets' destination; instead, packets are either dropped from the network or diverted to some other malicious nodes. Sinkhole attacks, which exhibit similar attack effects as blackhole attacks, can occur when the NoC supports adaptive routing. In this case, a malicious node actively solicits packets from its neighbor nodes by pretending to have sufficient free buffer slots. Effects and efficiencies of both sinkhole and blackhole DoS attacks are modeled and quantified in this paper, and a few factors that influence attack effects are found to be critical. Through fine-tuning of these parameters, both attacks are shown to cause more damages to the NoC, measured as over 30% increase in packet loss rate. Even with current detection and defense methods in place, the packet loss rate is still remarkably high, suggesting the need of new and more effective detection and defense methods against the enhanced blackhole and sinkhole attacks as described in the paper.

Keywords: networks-on-chip, hardware Trojan, denial-of-service attack

1. Introduction

Hardware Trojans (HT) can pose a serious threat to many-core chips, as they might cause the chips to malfunction, or leak sensitive information. HTs can be inserted by embedding a malicious circuit during the design or manufacturing phase of a chip [1]. In the literature [2, 3, 4], a few HT designs were proposed and they could be used to launch denial-of-service (DoS) attacks against the networks-on-chip (NoC) component of a many-core chip, and the HT-enabled DoS attacks can cause serious damages to NoC, including dropping of packets, jamming of certain network node(s), leaking sensitive information, or modification of functionalities, *etc.* [1].

In this paper, we consider two HT-assisted Denial-of-Service (DoS) attacks, namely sinkhole and blackhole attacks targeting NoC in a many-core chip. Both attacks can cause great damage to the chips and the users of the chips. For a balckhole attack, it can cause chips to malfunction and leak the sensitive information, while a sinkhole attack can aggregate the traffic and intercept the packets. In addition, the two attacks are easy to be realized by an HT that has extremely low area and power costs, and can be hard to detect.

To enable a blackhole attack, HTs are inserted into the routers such that packets are not forwarded to their intended destination; instead, the packets are either dropped out from the network or forwarded to other malicious nodes. Suppose node 1 in the example shown in Fig. 1 has a packet that needs to be sent to node 9, and the packet is routed through a malicious node, node 6. Upon receiving the packet, node 6 actually sends the packet to a malicious node, node 5 in this example. Node 9, the intended recipient of the packet, will not be able to receive a single packet from node 1. It should be noted that as there is only one malicious interceptor, and as so, there will be no deadlock in the network caused by the attack.

☆This research program is supported by the Natural Science Foundation of China No. 61376024 and 61306024, Natural Science Foundation of Guangdong Province 2015A030313743 and 2018A030313166, Special Program for Applied Research on Super Computation of the NSFC-Guangdong Joint Fund (the second phase), and the Science and Technology Research Grant of Guangdong Province No. 2016A010101011 and 2017A050501003, Pearl River S&T Nova Program of Guangzhou No. 201806010038, and Tip-top Scientific and Technical Innovative Youth Talents of Guangdong special support program (No. 2014TQ01X590).

*Corresponding author

Email addresses: 201721045909@mail.scut.edu.cn (Li Zhang), xiaohangwang@scut.edu.cn (Xiaohang Wang), yingtao.jiang@unlv.edu (Yingtao Jiang), mei.yang@unlv.edu (Mei Yang), tmak@ecs.soton.ac.uk (Terrence Mak), a.k.singh@essex.ac.uk (Amit Kumar Singh)

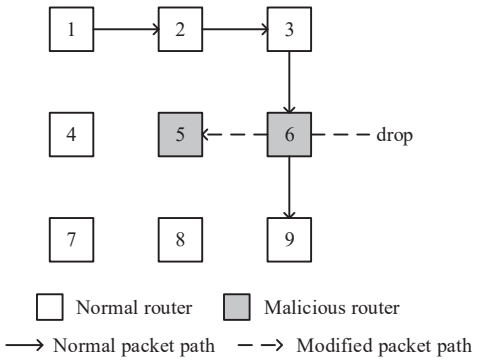


Figure 1: An example illustrating a blackhole attack.

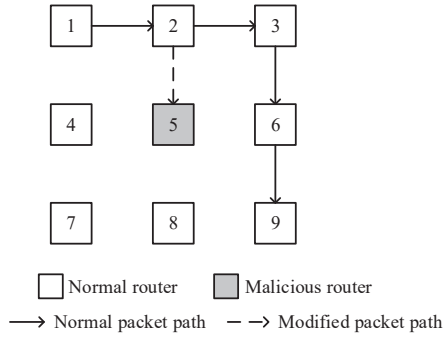


Figure 2: An example illustrating a sinkhole attack.

From the example shown in Fig. 1, one can see that in a blackhole attack, the malicious nodes passively drop packets or reroute packets to unintended recipients. This is quite different from a sinkhole attack, where a malicious node actively solicits packets from its neighbor nodes by pretending to have sufficient free input buffer slots with adaptive routing. To illustrate this type of attack, let us assume that node 1 in Fig. 2 needs to send a packet to node 9. When a packet reaches node 2, it has to make a decision regarding which of the two downstream routers, nodes 3 and 5, shall be forwarded to. This decision is largely determined by node 2's knowledge about how many input buffer slots that each of nodes 3 and 5 has. Node 5, a malicious router in this example, has purposely notified node 2 that it has more empty slots in its input buffer than node 3. As a result, a packet passing through node 2 will more likely be routed to node 5 than to node 3. This malicious node can then either drop any packet coming to it or forward a packet to some other nodes for more harm. Either way, node 9 will not be able to receive some or all the packets that were designated to it.

Effects of the above described sinkhole and blackhole DoS attacks depend on a number of factors, including the number of HTs and their distributions in the NoC, traffic characteristics of the applications, and a few system parameters. In this paper, we intend to study and model how these factors and parameters can be explored to enhance the effectiveness of attacks. We will also examine how well the current detection and defense methods respond to the enhanced blackhole and sinkhole attacks described in the paper.

The contribution of the paper is two-fold. First, we propose the HT-assisted blackhole and sinkhole attacks targeting NoC, which can be launched by an HT that is found hard to be detected. Design of the HT is thus described and the attack flow is presented. The stealthiness of the HT is also analyzed and guaranteed. Second, we explore the factors that correlate to the attack effects of sinkhole and blackhole attacks. A method to maximize the attack effects is presented, and correspondingly, an HT insertion methodology is proposed for maximized attack effects in different situations.

The rest of the paper is organized as follows. Section 2 reviews the related works. Realization of blackhole/sinkhole attacks is described in Section 3, followed by a detailed study on various parameters that can contribute to the attack effects in Section 4. Section 5 introduces the detection and defense methods that can be employed to thwart the sinkhole and blackhole DoS attacks. Section 6 reports the results and assesses the effectiveness of the two DoS attacks with or without detection/defense employed. Finally, Section 7 concludes the paper.

2. Related Work

2.1. Hardware Trojans

There are many possible channels that can get an HT into a chip. For instance, when a many-core chip design house employs a foundry to manufacture the chip, a compromised staff member of the foundry can secretly insert HTs to the chip layout before it is fabricated. Once the infected chips after manufacturing gets to end users' systems, a hacker can gain the access to the chip by activating the HTs in the chip. Designing and defending against HTs in a chip has been a hot research topic [2, 3, 4, 1, 5, 6]. Various HTs and countermeasures have been proposed [2, 7, 8, 9, 10, 11, 12]. A typical HT is made of the trigger, the Trojan circuit and the payload [1]. Hiding in the many-core chips, HTs often hibernate most of the time and wake up for specific signals or events [13]. Once a specific signal or an event is present, the trigger of an HT first activates, and then the payload circuit launches the attack. Such operational model makes an HT difficult to be detected during the design phase through computer simulations or by off-line testing without explicit knowledge of the specific signals or events that trigger the attacks [14]. Hardware Trojans may engage in different actions, including modifying the functionality or specification of the hardware, leaking sensitive information, or launching denial of service attacks [3, 13, 15, 16].

HTs can be categorized into combinational Trojans and sequential Trojans according to their triggering methods [5]. A combinational Trojan is activated by a set of specific signals, while a sequential Trojan requires a sequence

of specific events to trigger its payload. Based on the triggering condition, hardware Trojans can then be classified as logic-based, sensor-based and always-on Trojans [6]. In a logic-based Trojan, a specific binary pattern, say 00110101, in the payload of a data packet is reserved to activate the Trojan. A sensor-based Trojan, on the other hand, will be fired up by reaching certain temperature and power levels as determined by the on-chip sensors. An always-on Trojan, as its name suggests, is up running all the time, and it does not need a trigger.

Current countermeasures against HT attacks can be classified into three categories: HT prevention, HT detection and HT defense [1].

HT prevention is a practice that takes place during the chip design stage to prevent the insertion of HTs in the first place [17, 18].

HT detection relies on various approaches to determine the existence of HTs, and locate them if they do exist. In [19], a sustained vector methodology, where vectors are repeated multiple times at the inputs of both the genuine and the Trojan circuits, was proposed to help detect a Trojan that hides in a chip. Another study provided a proof-of-concept demonstration of the potential benefit of using logical implications for the detection of combinational hardware Trojans [20]. In [21], the authors concerned on the hardware Trojan detection in the network interfaces of networks-on-chip using the state obfuscation.

HT defense is a process that wipes out the HTs entirely, or at least, reduces the attack effects of the HTs. In [22], a method that attempts to detect the presence of Trojans by continuous monitoring and testing of the chip; if a core is found infected with an HT, this infected core will no longer be used and all its computing tasks will be switched over to some other core(s). Another method, path security (P-Sec) validation technique, was proposed to protect compromised networks-on-chip architectures from fault injection side channel attacks [23]. Traffic isolation, a method to reduce the latency incurred by partitioning, also can be used to protect against DoS and bandwidth attacks because of the static time allocation to different domains [24, 25].

2.2. HT-enabled DoS attacks on NoC

HT-assisted DoS attacks [26, 16, 27, 28, 29] can directly target the NoC of a many-core chip, as malfunctioning of NoC can cause the entire chip to be disconnected and disintegrated, even though each single core might still be fully functional. In [26], a bandwidth denial attack that increases the network latency by rejecting the resource request was described, and a detection method referred as RLAN (Runtime Latency Auditor for NoCs) was suggested. In a simple term, RLAN detects the HT when network latency is found abnormal. In [27], a DoS attack in wireless NoCs was launched by reducing normal nodes bandwidth and thus causing widespread bandwidth loss. The authors also proposed a DoS resilient wireless architecture to defend against such an attack, and they also suggested countermeasures that can alleviate the effect of the DoS attack with defense methods at both physical and data routing levels. In [28], various flooding-based DoS attacks were evaluated and the robustness of mesh-based NoC architectures under these attacks was examined. In [29], a target-activated sequential payload (TASP) HT in support of a new type of DoS attack was proposed. To circumvent the threat of HTs, the author proposed a heuristic threat detection model to classify faults and discover HTs within compromised links.

2.3. Blackhole and sinkhole DoS attacks

Blackhole and sinkhole attacks are two of the most severe attacks known for sensor networks [30, 31, 32, 33, 34, 35]. When a blackhole attack is launched, a malicious node captures data from its neighboring nodes and stops forwarding the data packets to their original destinations [33]. Such a malicious node is called as blackhole node and the region that encompasses such a node is known as the region of blackhole. To identify and mitigate the malicious nodes, in [33], route request packets are flooded across the network to create a reliable path between the source and the destination. In a sinkhole attack, the traffic is directed to the hostile node and then many attacks like selective and blackhole can be empowered by a sinkhole attack [35]. A sinkhole attack is shown to be detectable using the Delphi (Delay per Hop Indicator) technique as proposed in [35].

Although there have a lot of studies on blackhole and sinkhole attacks in the context of sensor networks, few consider these attacks in NoC and the design of hardware Trojans needed to launch and sustain such attacks. In [26], a DoS attack targeting the NoC was envisioned, bearing a great deal of similarity to such an attack ever seen in sensor networks. As a matter fact, the attacks described in [26] actually can be easily detected by comparing latencies of similar packets.

In the next sections, we shall exploit how to ensure the invisibility of the attack and assess attack effects. In addition, we shall show that how to maximize the attack effects by tuning a few critical parameters, such as number and distribution of HTs, and a few more.

3. HT Designs for Sinkhole/Blackhole Attacks

In this section, we provide an HT design that enables the sinkhole and blackhole DoS attacks. In Section 3.1, we analyze the configuration that an HT needs and provide details regarding the process of launching an attack. Section 3.2 provides the detailed design of the HT module, and the low degree of detectability of the designed HT is shown in Section 3.3.

An HT can be inserted into the pipeline of a credit-based virtual channel router [36], as shown in Fig. 3. An HT has two parts: (1) the main part, named the main HT, which is used to configure and perform the blackhole

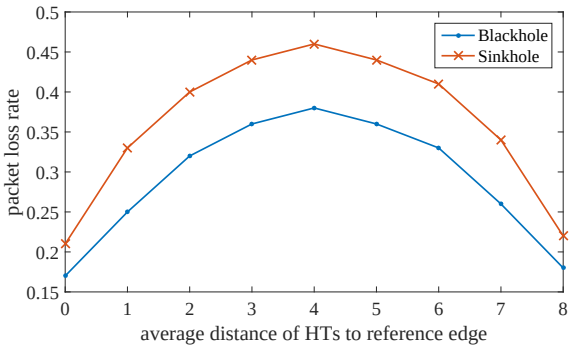


Figure 13: The average distance of HT to the reference edge vs. packet loss rate for blackhole and sinkhole attacks

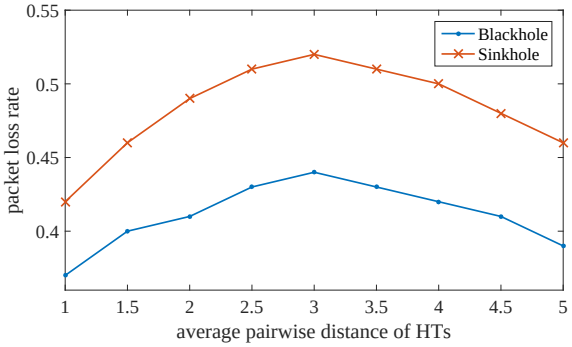


Figure 14: The average pairwise distance of HTs vs. packet loss rate for blackhole and sinkhole attacks

3, the packet loss rate declines. The reason is that when x_4 is small, the HTs are in close proximity. When HTs are scattered and are far away from each other, they may be close to the chip corners. In both cases, fewer packets travel through the HTs, and thus, fewer packets get dropped from the system. The sinkhole attack performs the similar result as blackhole attack and it's attack e□ect is better.

6.3.3. Path length of the packets

In this set of experiments, we set x_1 to be 5, x_3 to be 3, and x_4 to be 2. Fig. 15 shows the relationship between the average path length of packets (x_2) and the packet loss rate. From the Fig. 15, as the average path length increases, the packet loss rate increases in a nearly linear fashion. The reason is that, when the path length is long, there is a high probability that a packet may pass through a node infected with HT. The sinkhole attack performs the similar result as blackhole attack and it's attack e□ect is better.

6.4. Evaluating the attack e ects after optimization

We compare the attack e□ects of the optimized HT distribution by solving the optimization problem in Eqs. 3 and 4 (*e.g., with optimization*) and that of a random HT distribution (*i.e., without optimization*). In this set of experiments, the number of HTs varies from 1 to 6. The

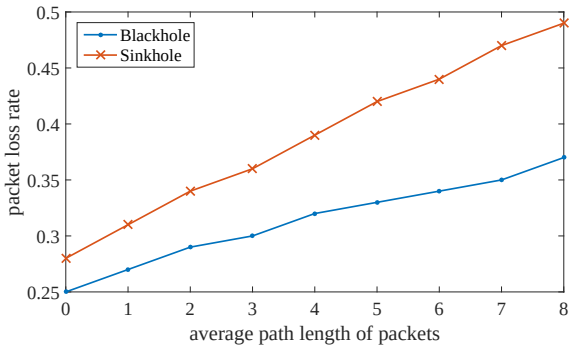


Figure 15: The average path length of packets vs. packet loss rate for blackhole and sinkhole attacks

average path length of the packet is set to be 2, 4, 8, respectively. Fig. 16(a)-(c) show the blackhole attack e□ects with and without optimization. The results are normalized to the case that the optimization is applied. One can see that the optimized HT distribution improves the attack e□ect by 30% compared to a random HT distribution, on average. From Fig. 16(a), when the average path length is 2 and the number of HTs is 1, the packet loss rate of the optimized HT distribution is 24% higher than that of the random HT distribution. From Fig. 16(c), when the average path length is 8 and the number of HTs is 3, the packet loss rate of the optimized HT distribution is 36% higher than that of the random HT distribution.

Fig. 17(a)-(c) compare the sinkhole attack e□ect with and without optimization. One can see that the optimized HT distribution improves the attack e□ect by 34% compared to the random HT distribution, on average. From Fig. 17(a), when the average path length is 2 and the number of HTs is 4, the packet loss rate of the optimized HT distribution is 25% higher than that of the random HT distribution. From Fig. 17(c), when the average path length is 8 and the number of HTs is 1, the packet loss rate of the optimized HT distribution is 41% higher than that of the random HT distribution.

6.5. Evaluating the defense methods

In this set of experiments, the number of chosen suspects varies from 2 to 10. The results are normalized to that of the case without applying any defense. Fig. 18(a) shows the packet loss rate caused by blackhole attack without and with defense measures deployed. One can see that packet loss rate in a system with defense employed is reduced by 42% on average. Even with more nodes being selected as the suspects and checked, the packet loss rate is still quite high, at 52% of the original. This is because when the HT changes its attack target, the detection method is no longer considered e□ective.

Fig. 18(b) shows the packet loss rates caused by sinkhole attack in both cases without and with defense. One can see that the packet loss rate of the case that employs defense is reduced by 39% on average. Even with more

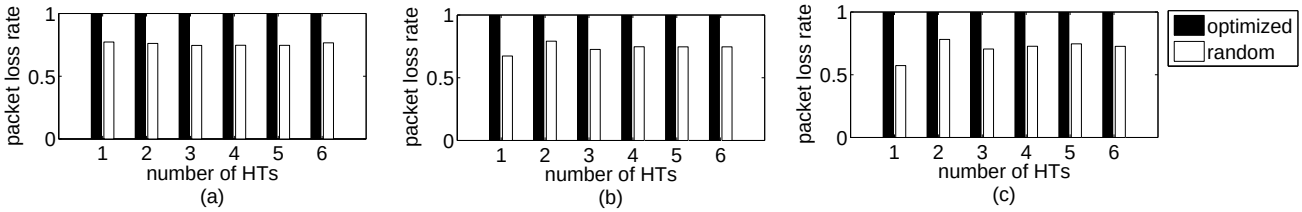


Figure 16: The packet loss rate comparison between the optimal HT distribution and random HT distribution for blackhole attack when average packet path length is (a) 2, (b) 4, (c) 8.

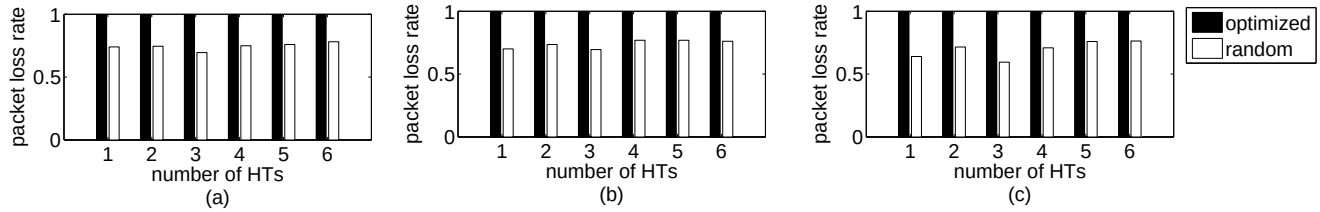


Figure 17: The packet loss rate comparison between the optimal HT distribution and random HT distribution for sinkhole attack when average packet path length is (a) 2, (b) 4, (c) 8.

nodes being selected as the suspects, the packet loss rate remains high, at 57% of the original. In a simple word, the effectiveness of the current detection and defense against the enhanced blackhole and sinkhole attacks, as described in Section 5, tends to be quite limited.

As alluded before, the configuration module can help change the trigger conditions. When the attack target and attack interval are changed, the detection method makes little effect because they fail to trigger the HTs.

7. Conclusion

Blackhole/sinkhole DoS attacks targeting the NoC systems of many-core chips can cause severe packet losses and/or divert traffic to malicious nodes other than their intended designations. In this paper, the effects of the attacks as measured by packet loss rate, were quantitatively modeled by considering several critical parameters, including number of HTs and their distribution in NoC. Through fine-tuning of these parameters, both attacks are shown to cause more damages to NoC, with the packet loss rate jumped by more than 30%. Even with detection and defense methods in place, the packet loss rate can still reach 52%. This research indicates a strong need to develop more effective countermeasures to thwart these enhanced attacks.

References

[1] H. Li, Q. Liu, J. Zhang, A survey of hardware Trojan threat and defense, Integration, the VLSI Journal 55 (2016) 426–437.

[2] D. M. Shila, V. Venugopal, Design, implementation and security analysis of hardware Trojan threats in FPGA, in: Proc. IEEE Int'l Conf. Communications, 2014, pp. 719–724.

[3] R. S. Chakraborty, S. Narasimhan, S. Bhunia, Hardware Trojan: Threats and emerging solutions, in: Proc. IEEE Int'l High Level Design Validation and Test Workshop, 2009, pp. 166–171.

[4] Y. Jin, N. Kupp, Y. Makris, Experiences in hardware Trojan design and implementation, in: Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust, 2009, pp. 50–57.

[5] S. Bhunia, M. S. Hsiao, M. Banga, S. Narasimhan, Hardware Trojan attacks: threat analysis and countermeasures, IEEE J. Proc. IEEE 102 (8) (2014) 1229–1247.

[6] M. Tehranipoor, F. Koushanfar, A survey of hardware Trojan taxonomy and detection, IEEE Design Test of Computers 27 (1) (2010) 10–25.

[7] Y. Jin, Y. Makris, Hardware Trojan detection using path delay fingerprint, in: Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust, 2008, pp. 51–57.

[8] X. Wang, H. Salmani, M. Tehranipoor, J. Plusquellic, Hardware trojan detection and isolation using current integration and localized current analysis, in: Proc. IEEE Int'l Symp. Defect and Fault Tolerance VLSI Systems, 2008, pp. 87–95.

[9] M. R. Kakoee, V. Bertacco, L. Benini, A distributed and topology-agnostic approach for on-line NoC testing, in: Proc. ACM/IEEE Int'l Symp. Networks-on-Chip, 2011, pp. 113–120.

[10] S. Bhasin, F. Regazzoni, A survey on hardware trojan detection techniques, in: Proc. IEEE Int'l Symp. Circuits and Systems, 2015, pp. 2021–2024.

[11] B. Cha, S. K. Gupta, A resizing method to minimize effects of hardware Trojans, in: Proc. IEEE Symp. Asian Test, 2014, pp. 192–199.

[12] M. Banga, M. S. Hsiao, A region based approach for the identification of hardware Trojans, in: Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust, 2008, pp. 40–47.

[13] J. H. G. S. N Jacob, D Merli, Hardware Trojans: current challenges and approaches, IET Computers and Digital Techniques 8 (6) (2014) 264–273.

[14] S. M. J. M.Hicks, M.Finnicum, Overcoming anuntrusted computing base: detecting and removing malicious hardware automatically, in: Proc. IEEE Symp. Security and Privacy, 2010, pp. 159–172.

[15] C. Reinbrecht, A. Susin, L. Bossuet, G. Sigl, J. Sepuveda, Side channel attack on NoC-based MPSoCs are practical: NoC Prime+Probe attack, in: Proc. Symp. Integrated Circuits and Systems Design(SBCCI), 2016, pp. 1–6.

[16] A. Malekpour, R. Ragel, A. Ignjatovic, S. Parameswaran, DoSGuard: Protecting pipelined MPSoCs against hardware Trojan based DoS attacks, in: Proc. IEEE Int'l Conf. Application-specific Systems, Architectures and Processors(ASAP), 2017, pp. 45–52.

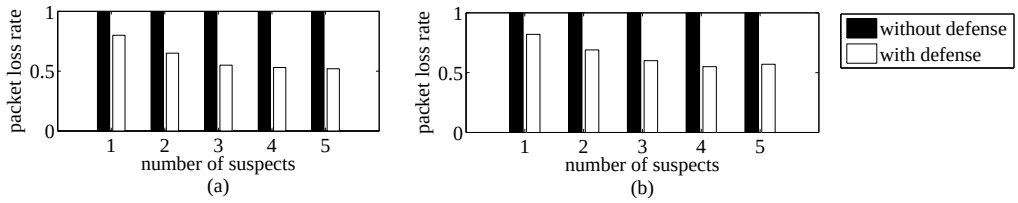


Figure 18: Comparison of the packet loss rate with and without defense methods, for the (a) blackhole attack, and (b) sinkhole attack.

[17] Q. Yu, J. Dofe, Z. Zhang, Exploiting hardware obfuscation methods to prevent and detect hardware Trojans, in: Proc. IEEE Int'l Midwest Symposium on Circuits and Systems (MWSCAS), 2017, pp. 819–822.

[18] K. Xiao, D. Forte, M. Tehranipoor, A Novel Built-In Self-Authentication Technique to Prevent Inserting Hardware Trojansg, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33 (12) (2014) 1778–1791.

[19] H. M. S. Banga M, A novel sustained vector technique for the detection of hardware Trojans, in: Proc. IEEE Int'l Conf. VLSI Design, 2009, pp. 327–332.

[20] N. Cornell, K. Nepal, Combinational hardware Trojan detection using logic implications, in: Proc. IEEE Int'l Midwest Symposium on Circuits and Systems (MWSCAS), 2017, pp. 571–574.

[21] J. Frey, Q. Yu, Exploiting state obfuscation to detect hardware trojans in NoC network interfaces, in: Proc. Int'l Midwest Symp. Circuits and Systems, 2015, pp. 1–4.

[22] A. Malekpour, R. Ragel, A. Ignjatovic, S. Parameswaran, TrojanGuard: Simple and e□ective hardware Trojan mitigation techniques for Pipelined MPSoCss, in: Proc. Design Automation Conference (DAC), 2017, pp. 1–6.

[23] T. Boraten, A. K. Kodi, Packet security with path sensitization for NoCs, in: Proc. Design, Automation Test Europe Conf. Exhibition, 2016, pp. 1136–1139.

[24] H. M. G. Wassel, Y. Gao, J. K. Oberg, T. Hu□mire, R. Kastner, F. T. Chong, T. Sherwood, SurfNoC: A low latency and provably non-interfering approach to secure networks-on-chip, in: Proc. Symp. Int'l Symp. Computer Architecture(ISCA), 2013, pp. 296–310.

[25] A. Psarras, J. Lee, I. Seitanidis, C. Nicopoulos, G. Dimitrakopoulos, PhaseNoC: Versatile network tra□c isolation through TDM-Scheduled virtual channels, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 35 (5) (2016) 844–857.

[26] R. JS, D. M. Ancajas, K. Chakraborty, S. Roy, Runtime detection of a bandwidth denial attack from a rogue network-on-chip, in: Proc. Int'l Symp. Networks-on-Chip, 2015, pp. 8:1–8:8.

[27] A. Ganguly, M. Y. Ahmed, A. Vidapalapati, A denial-of-service resilient wireless NoC architecture, in: Proc. the Great Lakes Symp. VLSI, 2012, pp. 259–262.

[28] D. Fang, H. Li, J. Han, X. Zeng, Robustness analysis of mesh-based network-on-chip architecture under flooding-based denial of service attacks, in: Pro. IEEE Int'l Conf. Networking, Architecture and Storage, 2013, pp. 178–186.

[29] T. Boraten, A. K. Kodi, Mitigation of denial of service attack with hardware Trojans in NoC architectures, in: Proc. IEEE Int'l Symp. Parallel and Distributed Processing, 2016, pp. 1091–1100.

[30] C. Karlof, D. Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks 1 (2) (2003) 293–315.

[31] D. R. Raymond, S. F. Midki□, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervasive Computing 7 (1) (2008) 74–81.

[32] A.-S. K. Pathan, H.-W. Lee, C. S. Hong, Security in wireless sensor networks: issues and challenges, in: Proc. Int'l Conf. Advanced Communication Technology, Vol. 2, 2006, pp. 6–pp.

[33] H. Kaur, A. Singh, Identification and mitigation of black hole attack in wireless sensor networks, in: Proc. Int'l Conf. Micro-Electronics and Telecommunication Engineering (ICMETE), 2016, pp. 616–619.

[34] M. U. Farooq, X. Wang, R. Yasrab, S. Qaisar, Energy preserving detection model for collaborative black hole attacks in wireless sensor networks, in: Proc. Int'l Conf. Mobile Ad-Hoc and Sensor Networks (MSN), 2016, pp. 395–399.

[35] M. Kaur, A. Singh, Detection and mitigation of sinkhole attack in wireless sensor network, in: Proc. Int'l Conf. Micro-Electronics and Telecommunication Engineering (ICMETE), 2016, pp. 217–221.

[36] L.-S. P. Natalie Enright Jerger, Tushar Krishna, On-chip networks, second edition, Synthesis Lectures on Computer Architecture, 2017.

[37] S. I. Dimitrakopoulos G, Psarras A, Microarchitecture of network-on-chip routers, Springer, 2015.

[38] S. H.-L. M Snir, S Otto, J. Dongarra, MPI–the complete reference: the MPI core, MIT press, 1998.

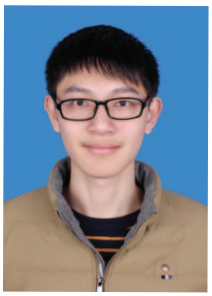
[39] M. Kayaalp, N. Abu-Ghazaleh, D. Ponomarev, A. Jaleel, A high-resolution side-channel attack on last-level cache, in: Proc. Design Automation Conference (DAC), 2016, pp. 72:1–72:6.

[40] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar, Trojan detection using IC fingerprinting, in: Proc. Symp. Security and Privacy(SP), 2007, pp. 296–310.

[41] T. Hastie, R. Tibshirani, J. Friedman, T. Hastie, J. Friedman, R. Tibshirani, The elements of statistical learning, Springer, 2009.

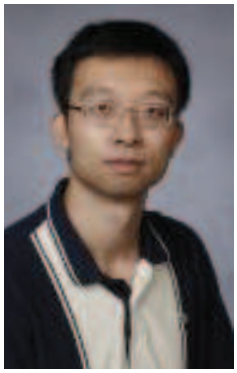
[42] C. J. Glass, L. M. Ni, The Turn model for adaptive routing, in: Proc. Ann. Int'l Symp. Computer Architecture, 1992, pp. 278–287.

Biography



Li Zhang received the bachelor's degree in software engineering from South China University of Technology, Guangzhou, China. He is working toward the master's degree in the school of software engineering, South China University of Technology. His research interests include hardware security, and NoC-based systems.

Xiaohang Wang received the B.Eng. and Ph.D degree in communication and electronic engineering from Zhejiang University, in 2006 and 2011. He is currently an associate professor at South China University of Technology. He was the receipt of PDP 2015 and VLSI-SoC 2014 Best Paper Awards. His research interests include many-core architecture, power e□cient architectures, optimal control, and NoC-based scystems.



Yingtao Jiang joined the Department of Electrical and Computer Engineering, University of Nevada, Las Vegas in Aug. 2001, upon obtaining his Ph.D degree in Computer Science from the University of Texas at Dallas. He has been a full professor since July 2013 at the same university, and now assumes the role of the Department Chair. His research interests include algorithms, computer architectures, VLSI, networking, nano-technologies, etc.

Mei Yang received her Ph. D. in Computer Science from the University of Texas at Dallas in Aug. 2003. She has been a full professor in the Department of Electrical and Computer Engineering, University of Nevada, Las Vegas since 2016. Her research interests include computer architectures, networking, and embedded systems.

Terrence Mak is an Associate Professor at Electronics and Computer Science, University of Southampton. Supported by the Royal Society, he was a Visiting Scientist at Massachusetts Institute of Technology during 2010, and also, a□liated with the Chinese Academy of Sciences as a Visiting Professor since 2013. Previously, He worked with Turing Award holder Prof. Ivan Sutherland, at Sun Lab in California and has awarded Croucher Foundation scholar. His newly proposed approaches, using runtime optimisation and adaptation, strengthened network reliability, reduced power dissipations and significantly improved overall on-chip communication performances. Throughout a spectrum of novel methodologies, including regulating tra□c dynamics using networks-on-chip, enabling unprecedented MTBF and to provide better on-chip e□ciencies, and proposed a novel garbage collections methods, “defragmentation”, together led to three prestigious best paper awards at DATE 2011, IEEE/ACM VLSI-SoC 2014 and IEEE PDP 2015, respectively. More recently, his newly published journal based on 3D adaptation and deadlock-free routing has awarded the prestigious 2015 IET Computers & Digital Techniques Premium Award. He has published more than 100 papers in both conferences and journals and jointly published 4 books.

Amit Kumar Singh received the B.Tech. degree in Electronics Engineering from Indian Institute of Technology (Indian School of Mines), Dhanbad, India, in 2006, and the Ph.D. degree from the School of Computer Engineering, Nanyang Technological University(NTU), Singapore, in 2013. He was with HCL Technologies, India for year and half before starting his PhD at NTU, Singapore, in 2008. He worked as a post-doctoral researcher at National University of Singapore (NUS) from 2012 to 2014 and at University of York, UK from 2014 to 2016. Currently, he is working as senior research fellow at University of Southampton, UK. His current research interests include system level design-time and run-time optimizations of 2D and 3D multi-core systems with focus on performance, energy, temperature, and reliability. He has published over 45 papers in the above areas in leading international journals/conferences.