Exploring On-Chip Power Delivery Network Induced Analog Covert Channels

Longfei Wang[1], S. Karen Khatamifard[2], Ulya R. Karpuzcu[2], Selçuk Köse[1]
[1]Department of Electrical and Computer Engineering, University of Rochester
[2]Department of Electrical and Computer Engineering, University of Minnesota

1 Introduction

On-chip power delivery network is an essential part of modern integrated circuits. With a sophisticated control by the power management unit, an off-chip voltage level is converted and regulated to a dedicated voltage applicable to the on-chip load circuits. Meanwhile, high power conversion efficiency is maintained as load current changes. Components of a representative on-chip power delivery network [1, 2, 3, 4, 5, 6, 7, 8, 9] are shown in Figure 1. Within this network, output voltage of an off-chip voltage converter is supplied to the global power grid through VDD C4 pads. The inputs of on-chip voltage regulators (VRs) are connected to the global power grid and the outputs of on-chip VRs are connected to the local power grids. Global ground distribution supplies the ground plane and is connected to the package through GND C4 pads. Multiple voltage domains can be enabled by the distributed VRs providing disparate local power grids. Significant amount of work has been performed to demonstrate potential security vulnerabilities of shared resources within multi/many-core processors. One of these inevitably shared resources is the constituent of the power management and delivery subsystem such as the global power grid shown in Figure 1. Our recent works [10, 11] reveal a new covert channel due to shared power budget enforced by hierarchical on-chip power management. In this article, a previously unexplored, novel class of analog covert channel leveraging switching noise modulation is uncovered. The threat model and related mechanisms to form the covert communication are detailed and proof of concept results are provided.

2 Threat Model

Covert channels make leakage of sensitive information possible even when there is no designated media for transmission of such information [12]. The transmitting and receiving end can be, respectively, referred to as the source

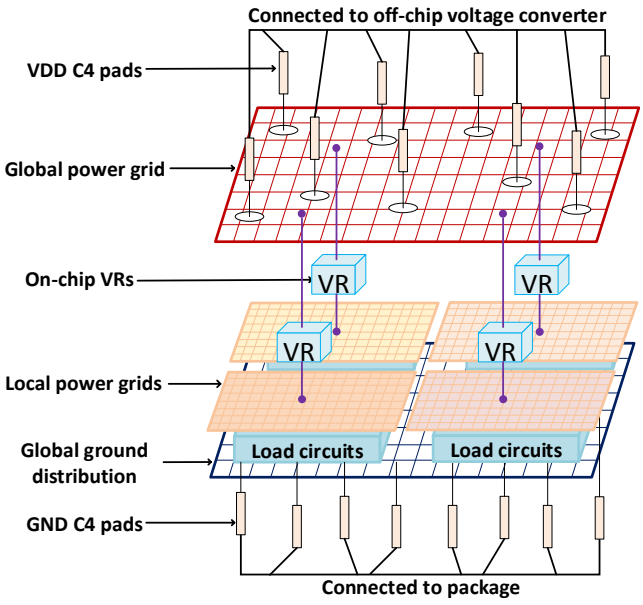

Figure 1: On-chip power delivery network.

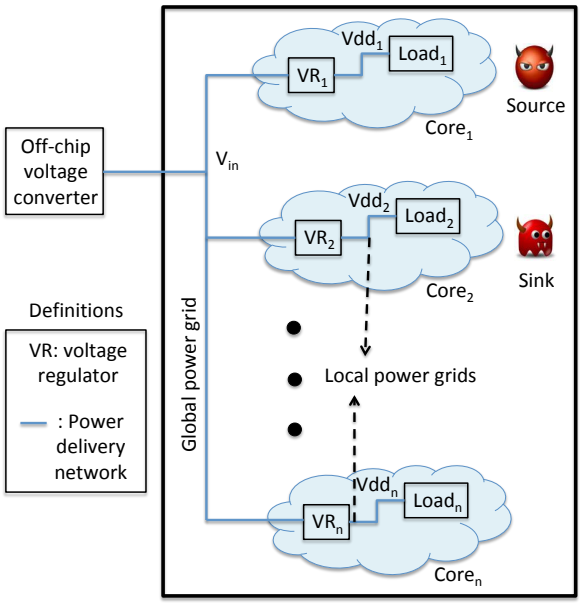

Figure 2: Power delivery network induced covert channel.

and sink. Both the source and sink can be either hardware components or software components sharing hardware resources [13]. The source is assumed to have access to the sensitive information but not to the network, which can be accessed by third parties. On the other hand, the sink is assumed to be capable of transmitting information through the network but have no access to the sensitive information. Due to the existence of covert channels, the sensitive information can be transmitted from the source to the sink and further to the third parties through the network. The covert communication, however, is not apparent to the hardware and software layers residing in the same system. In this article, on-chip VRs are considered as the source and sink. Covert communication is established through the shared global power grid.

3 Proof of Concept Results

As a proof of concept example, a power delivery network consisting of an off-chip VR and multiple on-chip VRs is considered, as shown in Figure 2. The output voltage of the off-chip VR is connected to the global power grid, which supplies the inputs of the on-chip VRs. There are n cores with each powered by an on-chip VR. The output of each on-chip VR is connected to a local power grid providing the supply voltage of the load circuit within that specific core. It is assumed that the sink core is idle while the source core is active when covert channel needs to be established. Without loss of generality, low-dropout (LDO) regulators are implemented as the on-chip VRs for this example. LDOs similar to [5] are adopted and an RC chain model is utilized for the power grid. Power grid parameters from [14] are applied. The activity of the source is modeled as a transient current at the output of VR_1 with the pattern decided by a random bit stream. When there is no covert communication, the load current of VR_1 consists of some leakage current and this transient current. When sensitive information needs to be transmitted from the source to the sink, a periodic current encoding the information will be added to $Load_1$. Meanwhile, as the sink is idle, the load current of VR_2, $Load_2$, only carries a small transient current and some leakage current. Due to the added periodic current to $Load_1$, fluctuations at the input of VR_1 are introduced as the control loop of VR_1 begins to respond. Such fluctuations also occur at the input of VR_2 due to the shared global power grid. The control loop of VR_2 also responds to maintain a constant supply voltage Vdd_2.

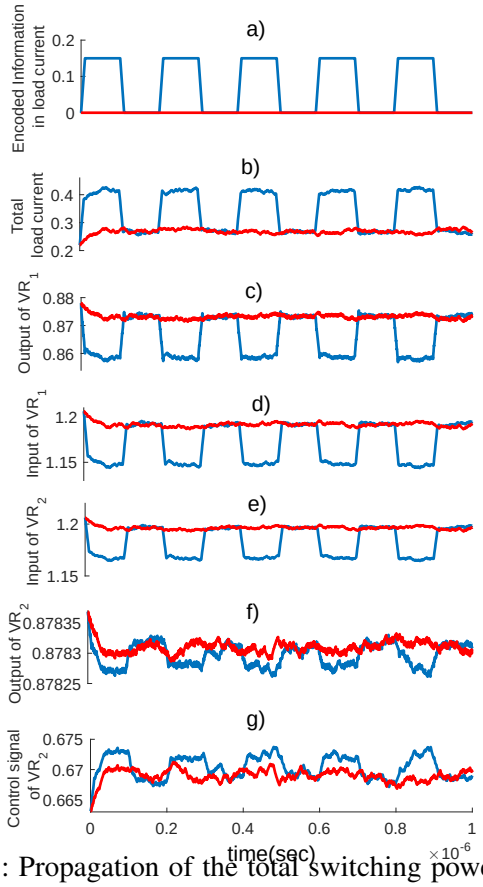

Figure 3: Propagation of the total switching power noise from source to sink over the global power delivery network with intentional noise (i.e., encoded information leak) shown in blue and without intentional noise shown in red.

The transmission of the voltage fluctuations from the source to the sink core is simulated in Cadence according to the above discussion utilizing a 45nm CMOS process. The simulation results with and without intentional noise are demonstrated in Figure 3 with, respectively, blue and red lines. The encoded information reflected in the load current of the source is shown in Figure 3a. The total load current of the source is shown in Figure 3b. The output of VR_1 experiences fluctuations due to the periodically switching load current as featured in Figure 3c which in turn lead to fluctuations at the input of VR_1 as shown in Figure 3d. Such fluctuations can further propagate to the input of VR_2 through the shared global power grid as can be seen from Figure 3e. This intentional noise generated at the output of VR_1 results in some fluctuations at the output of VR_2 seen from Figure 3f. The control signal of

VR_2, which is visible to both the local and global controllers in a hierarchical power management system, is also highly affected by the encoded information due to the tight integration of the power delivery network that consists of the distributed VRs as demonstrated in Figure 3g. As supported by the preliminary data, the sensitive information encoded in the form of a switching load current at the output of an on-chip VR can propagate through the global power grid and be sensed by the local power controller of the other cores. Considering the digital control of on-chip VRs that is implemented in state-of-the-art integrated systems, sensitive information carried by the control signal of the on-chip VR at the sink side can be processed digitally without dedicated hardware.

4 Discussions

This proof-of-concept demonstrates the crucial need for security-aware design of on-chip power delivery network. As the number of voltage regulators that co-reside on a single die increases, the distributed power delivery networks require tighter integration which leads to the increased number of shared resources such as capacitors (be it flying or decoupling), inductors, and most importantly the local and global power/ground interconnection network. Additionally, the design of each individual VR becomes more complicated due to the challenges such as reliability, stability, power efficiency, response time, area, and workload-awareness. Each additional feature to tackle any of these challenges would potentially make the power delivery network more vulnerable against covert communication attacks similar to those explored in this paper. We claim that security should be included within these challenges early in the design process not only at the system or architectural level but also at the low level (analog/mixed signal/digital) circuit design.

5 Conclusions

On-chip power delivery network provides regulated voltage levels to the load circuits while at the same time is vulnerable to information leakage through shared resources. A power delivery network induced analog covert channel enabled by shared global power grid and switching noise modulation is investigated in this article. Due to the strong correlation between the input and output of on-chip VRs, fluctuations can be introduced at the input of VR at the source side due to added switching load current. Such fluctuations propagate through the shared global power grid and are finally sensed by the local power control circuitry of the other cores. Proof of concept results for the on-chip power delivery network induced analog covert channel are demonstrated through Cadence simulations. Increased design complexity and shared resources necessitate inclusion of security features at the early design stage.

6 Acknowledgement

This work is supported in part by the NSF CAREER Award under Grant CCF-1350451, in part by the NSF Award under Grant CNS-1715286, in part by SRC Contract NO: 2017-TS-2773, and in part by the Cisco Systems Research Award.

References

[1] I. Vaisband, R. Jakushokas, M. Popovich, A. V. Mezhiba, S. Köse, and E. G. Friedman, *On-Chip Power Delivery and Management, Fourth Edition.* Springer, 2016.

[2] S. B. Nasir, Y. Lee, and A. Raychowdhury, "Modeling and Analysis of System Stability in a Distributed Power Delivery Network with Embedded Digital Linear Regulators," *Proceedings of the IEEE International Symposium on Quality Electronic Design (ISQED)*, pp. 68-75, February 2019.

[3] J. F. Bulzacchelli, Z. Toprak-Deniz, T. M. Rasmus, J. A. Iadanza, W. L. Bucossi, S. Kim, R. Blanco, C. E. Cox, M. Chhabra, C. D. LeBlanc, C. L. Trudeau, and D. J. Friedman, "Dual-Loop System of Distributed

Microregulators with High DC Accuracy, Load Response Time Below 500 ps, and 85-mV Dropout Voltage," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 4, pp. 863-874, April 2012.

[4] P. Zhou, D. Jiao, C. H. Kim, and S. S. Sapatnekar, "Exploration of On-Chip Switched-Capacitor DC-DC Converter for Multicore Processors using a Distributed Power Delivery Network," *Proceedings of the IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1-4, September 2011.

[5] S. Lai, B. Yan, and P. Li, "Localized Stability Checking and Design of IC Power Delivery with Distributed Voltage Regulators," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 32, no. 9, pp. 1321-1334, September 2013.

[6] W. Yu and S. Köse, "Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 2, pp. 244-257, April-June 2018.

[7] W. Yu, O. A. Uzun, and S. Köse, "Leveraging On-Chip Voltage Regulators as a Countermeasure Against Side-Channel Attacks," *Proceedings of the 52nd Annual Design Automation Conference*, pp. 1-6, June 2015.

[8] O. A. Uzun and S. Köse, "Converter-Gating: A Power Efficient and Secure On-Chip Power Delivery System," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 2, pp. 169-179, June 2014.

[9] L. Wang, S. K. Khatamifard, O. A. Uzun, U. R. Karpuzcu, and S. Köse, "Efficiency, Stability, and Reliability Implications of Unbalanced Current Sharing among Distributed On-Chip Voltage Regulators," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 11, pp. 3019-3032, November 2017.

[10] S. K. Khatamifard, L. Wang, S. Köse, and U. R. Karpuzcu, "POWERT Channels: A Novel Class of Covert Communication Exploiting Power Management Vulnerabilities," *Proceedings of the IEEE International Symposium on High-Performance Computer Architecture (HPCA)*, February 2019.

[11] S. K. Khatamifard, L. Wang, S. Köse, and U. R. Karpuzcu, "A New Class of Covert Channels Exploiting Power Management Vulnerabilities," *IEEE Computer Architecture Letters (CAL)*, vol. 17, no. 2, pp. 201 - 204, July - December 1 2018.

[12] Department of Defense Trusted Computer System Evaluation Criteria (Orange Book), December 26, 1985.

[13] H. Ritzdorf, "Analyzing Covert Channels on Mobile Devices," M.S. Thesis, ETH, 2012.

[14] R. Zhang, K. Wang, B. H. Meyer, M. R. Stan, and K. Skadron, "Architecture Implications of Pads as a Scarce Resource," *Proceedings of the 41st Annual International Symposium on Computer Architecture (ISCA)*, pp. 373-384, June 2014.