Sensing CPU voltage noise through Electromagnetic Emanations

Zacharias Hadjilambrou[¥], Shidhartha Das[*], Marco A. Antoniades[¥], Yiannakis Sazeides[¥]

[¥]University of Cyprus [*]ARM

Abstract— This work proposes sensing CPU voltage noise through wireless sensing of electromagnetic (EM) emanations from the CPU. Compared to previous voltage monitoring methodologies, this approach is not intrusive as it does not require direct physical access to the monitored CPU. To prove the effectiveness of this approach, we use EM signal feedback to find the resonant frequency of the CPU power delivery network, and to generate a CPU voltage noise (dI/dt) virus. This study is performed on a modern out-of-order CPU that supports on-chip fine grain voltage monitoring. This on-chip voltage monitoring capability is used to validate the proposed EM methodology.

Index Terms— Hardware reliability, voltage noise, electromagnetic emanations, stress tests

1 Introduction

Voltage noise forces CPU designers to set pessimistic voltage margins [1,2,7]. This limits the energy efficiency of modern CPUs. Fine grain voltage monitoring and voltage noise (dI/dt) stress tests are some of the main means used for developing techniques to mitigate the voltage noise detrimental ramifications. Monitoring allows better understanding of the voltage noise phenomena and dI/dt stress tests reveal weaknesses in the power-delivery network (PDN) to inductive transients. A combination of continuous monitoring and stress-test software enable the system-designer to explore the efficacy and correctness of design-margin mitigation techniques aimed at system-wide energy-efficiency improvements [2,5]. This work proposes a novel method for CPU voltage noise monitoring by sensing the voltage noise through EM emanations. This approach is unlike previous voltage sensing works that require direct physical access to the monitored CPU [1,2,5,6,16]. The paper also shows the effectiveness of the proposed scheme for crafting dI/dt stress tests.

In particular, this paper shows that by monitoring CPU EM emanations it is possible to: a) Detect voltage noise emergencies, b) Drive a genetic algorithm (GA) to converge towards a dI/dt virus by optimizing for maximum EM signal amplitude, and c) Find the resonant frequency of the CPU PDN. The study is performed on a modern out of order CPU that supports voltage noise monitoring through an on-chip circuit [5,6,16]. This on-chip voltage monitoring circuit is used to validate the EM methodology. The rest of the paper discusses the voltage noise phenomenon (Section 2), how CPU EM emanations can be detected and how voltage noise can be extracted from them (Section 3), the GA framework used for stress test generation (Section 4), the experimental details (Section 5), the experimental results (Section 6), related work (Section 7) and conclusions (Section 8).

2 Voltage Noise

The power delivery network is typically a distributed RLC network consisting of multiple LC-tank circuits [2,6] that manifest as multiple resonance frequencies. The highest resonance frequency (1st-order resonance) is attributed to on-die capacitance resonating with the package and/or the PCB inductance and is typically within the range of 50MHz - 200MHz. Power-supply oscillations with large magnitude are set off within the supply network as a result of a) abrupt transitions in the CPU current demand due to micro-architectural events such as branch mispredictions and cache-misses [1,5] and b) sustained program activity with alternating periods of high-current and low-current consuming instructions within a loop [2,16]. When the frequency of the time-varying current aligns closely with the 1st-order resonance frequency, power supply oscillations are maximized in amplitude, leading to bit-flips in SRAM storage arrays, timing errors in logic paths [1,2,7,16] and reliability issues due to gate-oxide stress [7,8]. Such periodic events often result in catastrophic execution failures through system/application crashes and/or incorrect execution output through silent data corruptions (SDCs).

References [2,6] provide more details on modern CPU PDNs and the PDN resonant frequency phenomena.

3 CPU EM Emanations – Why They Reveal Voltage Noise

It is known that CPUs emanate EM waves that can be captured using an antenna and a spectrum analyzer [9,10,15]. Periodic CPU activity due to program loops manifest as signal spikes on the spectrum analyzer. A loop that has a period T causes spectrum spikes that are visible on the spectrum analyzer at a frequency F equal to 1/T. These spikes are visible because of the differences in power drawn during the execution of the loop [9]. An easy way to cause visible spectrum spikes is to construct a loop that contains instructions that cause different CPU power consumption i.e. DIV and ADD. Changing the number of DIV or ADD instructions changes the fundamental frequency of the loop. Besides the fundamental frequency (F=1/T), instruction loops can have periodic events that repeat at frequencies higher than the fundamental frequency [6]. These events also manifest as EM spectrum spikes. By injecting instruction sequences into the CPU that cause periodic voltage noise fluctuations, this generates electric currents on the conductors and semi-conductors of the CPU, which in turn act as miniature antennas that transmit EM waves [17]. These EM emanations can then be received on the spectrum analyzer using a broadband antenna that operates in the frequency region of the emanations. It is proposed herein that the instruction sequences that cause large voltage noise fluctuations translate into transmitted EM waves with larger power levels, which manifest as signals with larger amplitudes on the spectrum analyzer. This hypothesis is validated in Section 6, where it is confirmed that high-amplitude EM signal spikes correlate with high voltage noise.

4 Genetic Algorithm Stress Test Generation Framework

Earlier studies show that GAs are useful for generating synthetic stress tests that maximize power consumption [3,4] and voltage noise [2,5]. GAs typically maximize a target metric by using operators inspired from biological evolution e.g. crossover (exchange of genes), mutation and selection of fittest individuals for breeding. Detailed explanations of how GAs work can be found in [12]. This work also utilizes GA for generating voltage noise stress test. This is the first work, though, that utilizes a GA driven by EM emanations for generating dI/dt virus. Our GA framework accepts as inputs assembly instructions along with desired loop size (in number of instructions) and attempts to find the mix and the order of instructions that maximizes the target metric. This paper uses two different target metrics: a) maximum droop that is observed using the readings of an on-chip voltage monitoring circuit, b) maximum EM signal amplitude that is measured through a spectrum analyzer. The viruses derived from GA search using the two metrics are compared in Section 6.5. The following GA parameters are empirically found to work well for our case study: a) loop size of 50 instructions, b) 2% mutation rate, c) one-point crossover, d) population size equal to 50 individuals and e) tournament selection is used for parent selection.

5 Experimental Details

As an experimental platform we used the JUNO R2 board [13]. This board offers a Cortex-A72 and Cortex-A53 big.LITTLE chip. An on-chip power supply monitor with an integrated digital storage oscilloscope (OC-DSO) [5,6,16] allows fine grain voltage readings of the Cortex-A72 cluster. For the rest of the paper we will refer to the on-chip oscilloscope as OC-DSO. The Cortex-A72 power domain consists of 2 cores and a last level cache (LLC). The OC-DSO makes this platform ideal for voltage noise research and validating the proposed EM methodology. For our study we keep idle the Cortex-A53 cluster and focus on capturing the EM signals emanated by the Cortex-A72 cluster. Figure 1 shows the experimental setup. An Agilent E4402B spectrum analyzer is used for measuring the EM signals. A broadband square loop antenna (3 cm side length) that operates in the range of 10 – 200 MHz was connected to the spectrum analyzer through a low-loss coaxial cable in order to receive the emanated waves from the JUNO board.

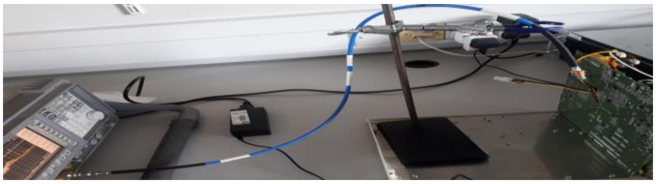

Figure 1. Experimental setup. The picture shows the following components: spectrum analyzer, cable, antenna and the JUNO board

6 Experimental Results

6.1 OC-DSO Characterization

First, we characterize the OC-DSO capability to monitor voltage correctly. Figure 2 shows voltage readings during three different scenarios: a) idle, b) during conventional benchmark execution (SPEC2006 gcc) and c) during dI/dt virus execution (virus is obtained using GA search with on-chip monitor). As expected, idle has the least amount of voltage noise, gcc execution produces slightly more noise and dI/dt virus causes massive voltage noise. As shown in Figure 6, gcc has higher Vmin (minimum operation voltage) than idle, and the virus has higher Vmin than gcc. This exercise shows that the OC-DSO reads voltage noise correctly and is a reliable tool for validating the EM methodology. Also, this exercise proves that the GA framework can successfully produce dI/dt viruses.

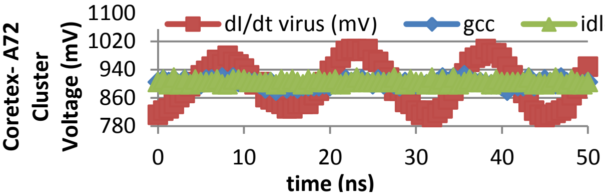

Figure 2. Voltage noise readings obtained by OC-DSO while running 3 different workloads

6.2 Measuring Resonant Frequency through Injecting Artificial Noise

This section determines the 1st order resonant frequency of the power delivery network of Cortex-A72 cluster through artificial noise injection [16]. More specifically, we load the Cortex-A72 PDN with a square-wave current pulse of known frequency using a synthetic current load (SCL) circuit integrated within the OC-DSO. A square-wave periodic current has an average DC component that is related to its amplitude and manifests as the average current draw from the load-circuit that can be measured externally. With the combined knowledge of the fundamental frequency of the square wave and its amplitude, we can accurately measure the amplitude of the fundamental frequency as shown in [16]. We sweep the fundamental frequency in the range between 10MHz and 130MHz (in steps of 1MHz) and measure the response of the PDN for each frequency step. In particular, we measure the maximum peak to peak supply voltage swing as a function of the fundamental frequency of excitation, as plotted in Fig. 3. The voltage swing maximizes at the 1st-order resonance frequency. For a distributed PDN, the peak impedance at the resonance frequency is relatively flatter (comparable magnitudes observed between 65-72MHz) compared to a canonical second-order LC tank circuit.

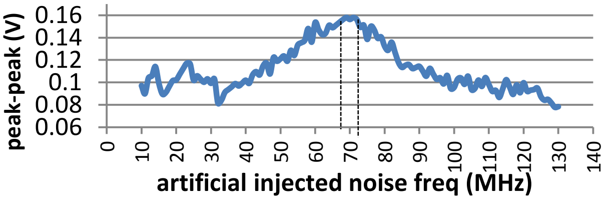

Figure 3. Artificial injected current swings at various frequencies reveal a resonant frequency in the range of 65-72MHz

For the rest of the paper any frequency in that range is considered as resonant frequency. It is worth noting that the dominant frequency (the one with the highest amplitude) of the virus used in Figure 2 falls in this range.

The results of this section are used next to validate the proposed EM methodology.

6.3 EM spikes correlation with voltage noise

To establish whether EM signal spikes correlate with voltage noise we perform Fast Fourier Transformation (FFT) of the OC-DSO voltage readings and compare the FFT results with the spectrum analyzer readings. Both readings are obtained at the same time while running a given program. The FFT converts the time domain voltage readings to the frequency domain that result in a series of signal amplitude vs frequency values. If these values match with the spectrum analyzer readings, then this is a strong indication that EM signals correlate with voltage noise. Figure 4 compares the spectrum analyzer readings with the FFT of OC-DSO voltage readings. The numbers are captured during the execution of a dI/dt virus that has a base loop frequency at 16.66MHz (60ns period), one dominant frequency at 66.66MHz (15ns) and causes some other visible spikes at 33, 50 and 84MHz. Both measurement methods (FFT of OC-DSO and spectrum analyzer) agree on the dominant frequency as well as on the other less dominant spikes. This suggests that EM signals are correlated with voltage noise. Note that the dominant frequency (the one with the highest amplitude) lies in the resonant frequency range determined in Section 6.2 to be 65-72MHz. This provides a strong indication that similarly to voltage noise, the EM signal amplitude is maximal at the resonant frequency.

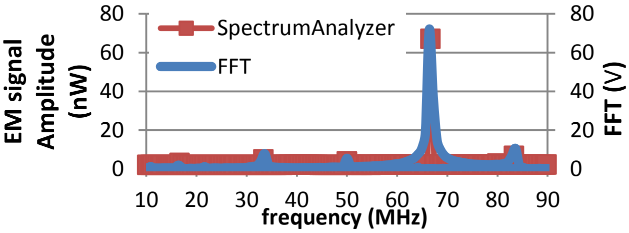

Figure 4. Comparison of spectrum analyzer readings (left axis) with FFT on OC-DSO voltage readings (right axis) during execution of a dI/dt virus. The two measurements agree as they reveal spikes at the same frequencies.

6.4 EM emanations driven GA

We run a GA search with target to maximize EM amplitude (in the frequency range of 10MHz-200MHz). The goal is to check how the generated EM based viruses correlate with on-chip voltage noise readings. Figure 5 clearly shows that as the signal amplitude increases from generation to generation during GA search the voltage droop increases as well.

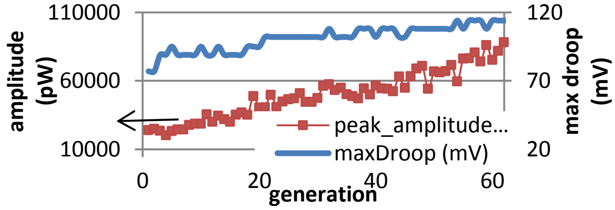

Figure 5. Peak amplitude (left axis) and maximum droop (right axis) for the best individual of each GA generation

Therefore, it is safe to say that GA search driven by EM signal amplitude essentially maximizes voltage noise. Also, it is observed (not shown in the graph for the sake of clarity and space constrains) that from the very first generations the GA prefers individuals that have dominant frequency in the area around the resonant frequency (65-72MHz). This confirms that voltage noise as well as EM signal amplitude is maximal at the resonant frequency.

6.5 Vmin tests

The ultimate test of how good is a voltage noise stress workload is its Vmin and how it compares to the Vmin of other non-viruses. Vmin represents the minimum operational voltage of a workload at a given CPU frequency. To demonstrate that EM driven GA is an effective methodology for generating stress tests that can be used for analyzing voltage margins, we compare the Vmin of the “EM virus” against the Vmin of SPEC2006 benchmarks, and against the Vmin of a GA virus driven by OC-DSO voltage readings (the standard approach for generating dI/dt viruses). Figure 6, shows the various Vmins as well as the maximum droop (obtained from the OC-DSO) caused by the various workloads. Both Cortex-A72 cores are active with each core running a separate instance of the workload. Each experiment is started at a high voltage and progressively voltage is lowered in steps of 10mV until a system crash. At each voltage step the workloads are run until completion and then check for SDC (by comparing the output against a golden reference obtained at a nominal operating point). Figure 6 reports the highest voltage at which any emergency occurred; an emergency means either SDC, application (APP) crash or system crash. We have observed (not shown in Fig. 6) that most workloads tend to show either SDC or application crash 10mV above the system crash. Both EM and OC-DSO viruses clearly cause higher voltage droop and have higher Vmin than the rest workloads. EM and OC-DSO virus are of equal strength. This proves that EM driven GA is feasible and reliable method for generating dI/dt viruses. For more confidence in the findings 30 Vmin tests are performed for each virus and two Vmin tests for each SPEC benchmark. In total the SPEC workloads run correctly for few dozen hours at voltages lower than the viruses’ Vmin.

It is worthwhile to mention that we have evaluated the proposed EM based dI/dt virus generation methodology on Cortex-A53 cluster with successful results. Due to space constrains we omit discussing these findings.

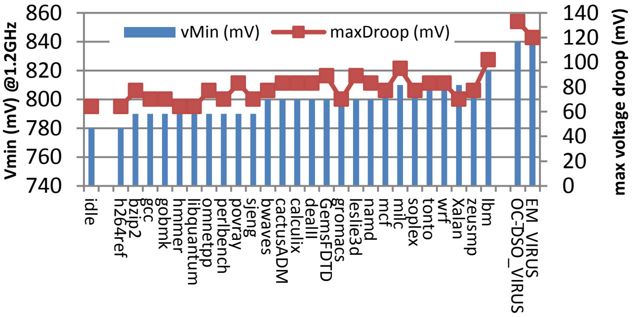

Figure 6. Vmin (blue bar, left axis) and maximum voltage droop (red curve, right axis) of various workloads for dual core runs. Viruses (rightmost workloads) cause higher droop and have higher Vmin than conventional benchmarks

6.6 EM methodology for finding the resonant frequency

As shown in Section 6.4, GA is able to find the resonant frequency and maximize the signal amplitude at that frequency, based only on external EM readings. This is quite useful but complex, in terms of time, as it requires 10s of GA generations and the whole GA search might require more than 24 hours to finish. In the case where the goal is only to determine the 1st resonant frequency, not to produce a dI/dt virus, an alternative faster method based on EM emanations is possible. The first step of this method is to design a simple loop of instructions that consists of two parts, a "high power" part and a "low power" part. This is required for causing a considerably high spectrum spike. The next step is to sweep the CPU frequency by changing the CPU clock and measure the EM signal amplitude. Sweeping the CPU frequency modulates the loop frequency. The hypothesis behind this method is that the CPU/ loop frequency with the highest amplitude should reveal the resonant frequency.

In a specific case-study, we used a loop with high part consisting of eight ADD instructions that are executed in 4 CPU cycles. And, a low part that consists of one DIV instruction that takes 4 CPU cycles to execute. Essentially, the difference in power arises from the fact that during the high power part, on average two instructions are executed per CPU cycle whereas during the low part, 0.25 instructions are executed per CPU cycle. The period of this loop at 1.2GHz CPU frequency is equal to 8ns which corresponds to a loop frequency of 150MHz. We sweep the CPU frequency from 1.2GHz until 120MHz. CPU frequency at 1.2GHz frequency corresponds to 150MHz loop frequency, 1.1GHz CPU frequency corresponds to 137.5MHz loop frequency, 1GHz frequency corresponds to 125MHz loop frequency etc. Figure 7, shows the results of such sweep. The amplitude is maximized at 72MHz which falls in the range of the 1st order resonant frequency (Section 6.2). We have also experimented with other loops with 6 and 7 cycle period. To increase or decrease the loop length we change the number of ADD pairs. The results (not shown due to space limitations) for all loops point to a resonant frequency in the range of 65-72MHz. This shows that the methodology can determine the resonant frequency with loops consisting of different instructions as long as they produce high enough EM signal amplitude.

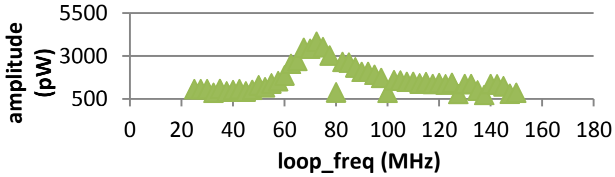

Figure 7. Loop frequency versus peak amplitude for a loop of 8 cycles. The loop frequency sweep is performed by modulating the CPU frequency. The figure reveals a resonant frequency at 72MHz.

7 Related Work

Previous work uses EM emanations to perform performance profiling [10], detect malicious activity [14] and perform side channel attacks [11,15]. This work utilizes EM emanations for monitoring voltage noise and designing dI/dt viruses. Earlier efforts utilized GA for generating dI/dt viruses using voltage noise direct chip measurements from external (through pins) [1,2] or internal (on-chip) oscilloscopes [5]. This work is the first to propose a method for obtaining dI/dt virus guided by EM signal amplitude measurements without requiring direct physical connection to the monitored CPU.

8 Conclusion

The proposed methodology for voltage noise monitoring has the advantage of not being intrusive in the sense that it does not require extra hardware on chip (e.g. OC-DSO), or cables connected to sense pins like an external oscilloscope would require. With the proposed EM methodology, voltage noise detection, resonant frequency characterization and dI/dt virus generation can virtually be performed on any CPU, even on those platforms that do not offer any external or internal voltage noise visibility. The proposed methodology also has the benefit that it can monitor multiple voltage domains at once e.g. in our experimental platform it is possible to monitor both the Cortex-A72 cluster and the Cortex-A53 cluster at the same time. For future work we plan to apply the EM methodology on other chips and platforms and to derive accurate models of dI/dt noise that correlate with microarchitectural activity.

Acknowledgment

This work is partially supported by European Union Horizon 2020 project Uniserver grant no. 688540 and the University of Cyprus.

References

[1] Reddi, Vijay Janapa, et al. "Voltage noise in production processors." IEEE micro 31.1 (2011): 20-28.

[2] Kim, Youngtaek, et al. "AUDIT: Stress testing the automatic way." Microarchitecture (MICRO), 2012 45th Annual IEEE/ACM International Symposium on. IEEE, 2012.

[3] Polfliet, Stijn, Frederick Ryckbosch, and Lieven Eeckhout. "Automated full-system power characterization." IEEE Micro 31.3 (2011): 46-59.

[4] Ganesan, Karthik, and Lizy K. John. "MAximum Multicore POwer (MAMPO): an automatic multithreaded synthetic power virus generation framework for multicore systems." Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis. ACM, 2011.

[5] Whatmough, Paul N., et al. "14.6 An all-digital power-delivery monitor for analysis of a 28nm dual-core ARM Cortex-A57 cluster." Solid-State Circuits Conference-(ISSCC), 2015 IEEE International. IEEE, 2015.

[6] Das, Shidhartha, Paul Whatmough, and David Bull. "Modeling and characterization of the system-level Power Delivery Network for a dual-core ARM Cortex-A57 cluster in 28nm CMOS." Low Power Electronics and Design (ISLPED), 2015 IEEE/ACM International Symposium on. IEEE, 2015.

[7] Reddi, Vijay Janapa, et al. "Voltage noise: Why it's bad, and what to do about it." 5th IEEE Workshop on Silicon Errors in Logic-System Effects (SELSE), Palo Alto, CA. 2009.

[8] Corbetta, S. et al. "System-Wide Reliability Analysis on Real Processor and Application under Vdd and T Stress", SELSE 2016

[9] Callan, Robert, et al. "A new approach for measuring electromagnetic side-channel energy available to the attacker in modern processor-memory systems." Antennas and Propagation (EuCAP), 2015 9th European Conference on. IEEE, 2015.

[10] Sehatbakhsh, Nader, et al. "Spectral profiling: Observer-effect-free profiling by monitoring EM emanations." Microarchitecture (MICRO), 2016 49th Annual IEEE/ACM International Symposium on. IEEE, 2016.

[11] Genkin, Daniel, et al. "Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation." International Workshop on Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg, 2015

[12] Mitchell, Melanie. An introduction to genetic algorithms. MIT press, 1998.

[13]http://infocenter.arm.com/help/topic/com.arm.doc.100114_0200_03_en/arm_versatile_express_juno_r2_development_platform_(v2m_juno_r2)_technical_reference_manual_100114_0200_03_en.pdf

[14] Nazari, Alireza, et al. "EDDIE: EM-Based Detection of Deviations in Program Execution." Proceedings of the 44th Annual International Symposium on Computer Architecture. ACM, 2017.

[15] Callan, Robert, Alenka Zajic, and Milos Prvulovic. "A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events." Microarchitecture (MICRO), 2014 47th Annual IEEE/ACM International Symposium on. IEEE, 2014.

[16] Whatmough, Paul N., et al. "Power Integrity Analysis of a 28 nm Dual-Core ARM Cortex-A57 Cluster Using an All-Digital Power Delivery Monitor." IEEE Journal of Solid-State Circuits 52.6 (2017): 1643-1654.

[17] Stutzman, Warren L., and Gary A. Thiele. Antenna theory and design. John Wiley & Sons, 2012.