On-Chip Sensor Circle Distribution Technique for Real-Time Hardware Trojan Detection

Selçuk Köse and Longfei Wang
Department of Electrical Engineering
University of South Florida
Tampa, Florida, United States 33620

Ronald F. DeMara
Department of Electrical Engineering and Computer Science
University of Central Florida
Orlando, Florida, United States 32816

Abstract: *Real-time hardware Trojan detection by monitoring voltage and current consumption using on-chip sensors is shown to be a feasible way to secure critical integrated circuit (IC) applications. This paper investigates the distribution and optimization of on-chip sensors for real-time hardware Trojan detection and localization based on the characteristics of on-chip power distribution network. On-chip voltage and current sensors are utilized to measure the voltage and current fluctuations and a new sensor placement scheme, circle distribution, is proposed to optimize the total number of sensors needed to locate hardware Trojans utilizing power grid characteristics as well as to estimate the hardware Trojan current. Simulation results verify that hardware Trojan activation can be effectively detected and located within the power grid and hardware Trojan current can be efficiently estimated with our proposed method.*

Keywords: Hardware Trojan; on-chip sensor optimization; power distribution network; power/ground noise.

Introduction

As IC technology advances, hardware security issues have been brought into great concern due to the fact that not all manufacturing steps of an IC are trustable. IC manufacturing steps accomplished in multiple companies can save cost while at the same time expose the ICs vulnerable to malicious modification of circuit parts known as hardware Trojans with the intent of degrading the circuit function or stealing confidential information from the circuit [1][2]. The need to develop an efficient hardware Trojan detection and isolation scheme becomes urgent especially for ICs with critical applications.

Several methods have been proposed for hardware Trojan detection. Real-time trust evaluation framework [3] can actively monitor Trojan activations and is shown to be effective to detect Trojan designed with advanced circuit techniques. Multiple power port measurements are performed in [4] for Trojan detection and isolation process and on-chip sensors are utilized in [5] to distribute across the chip to detect Trojan both with the help of a golden IC. These inspiring works can either detect Trojan in real time or estimate the location of Trojan, however, on-chip sensor coverage of the entire IC is needed for Trojan detection and optimum distribution of on-chip sensors or measurement points has not been investigated.

To more efficiently explore the powerful nature of real-time monitoring of ICs and on-chip sensor capabilities as well as to lay a foundation for Trojan deactivation by accurately locating the Trojan, an on-chip sensor circle distribution method is proposed for real-time hardware Trojan detection. This method utilizes the characteristics of on-chip power distribution network to optimize the distribution of sensors and to locate hardware Trojan. The main contributions of this paper are as follows: 1) Accurate real-time hardware Trojan detection and localization scheme using on-chip sensors. 2) Optimization of on-chip sensor distribution for hardware Trojan detection and location. 3) Hardware Trojan current estimation without the need for accurate current sensors.

Exploiting Power Noise to Detect Trojans

The fluctuations due to Trojan activity can be modeled as an additional current load shown in the circuit model of on-chip power grid in Fig. 1 (a) [6][7]. The voltage at an arbitrary node within the power grid can be expressed as [6][7]

$$V_{Node} = V_{supply} - \frac{1}{2}\sum_{i=1}^{n}[I_{load(i)} \times (R_{sn} + R_{sl(i)} - R_{nl(i)})] \quad (1)$$

where R_{sn}, R_{sl} and R_{nl} stand, respectively, for the effective resistance between the power supply and an arbitrary node, the effective resistance between the power supply and the load circuit, and the effective resistance between an arbitrary node and the load circuit.

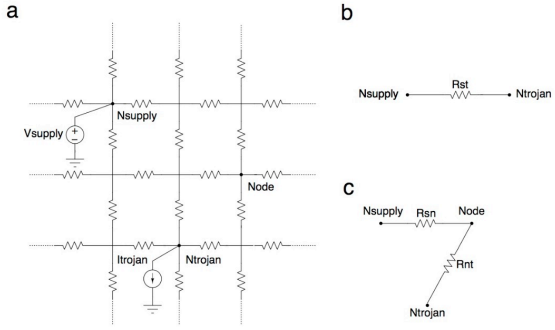


Figure 1. On-chip power grid model: (a) circuit model with power supply and Trojan, (b), (c) effective resistance between two nodes.

The voltage change at an arbitrary node within a power grid before and after Trojan is activated can be expressed as

$$\Delta V = -\frac{1}{2} I_{Trojan} \times (R_{sn} + R_{st} - R_{nt}) \tag{2}$$

where R_{st} and R_{nt} are corresponding effective resistances between two nodes as shown in Fig. 1 (b) and (c). By subtracting Trojan free voltage map, which can be obtained from a golden IC [3], [5], from the one with active Trojan, voltage fluctuations due to Trojan activation can be derived.

Proposed Circle Distribution of On-Chip Sensors

A closed form approximation of the effective resistance between any two points, $N_1(x_1, y_1)$ and $N_2(x_2, y_2)$ in the power distribution model with vertical and horizontal line resistances r_v and r_h where $r_h = kr_v$ is shown in [6][7] as below

$$\frac{R_{x,y}}{r} = \frac{\sqrt{k}}{2\pi}[\ln(x^2 + ky^2) + 3.44388] - 0.033425k - \frac{k(k-1)0.1975}{\pi}, \tag{3}$$

where $x = |x_1-x_2|$, $y=|y_1-y_2|$, $r_v=r$, $r_h = kr$. For a uniform power power grid where k = 1, (3) can be simplified as

$$\frac{R_{x,y}}{r} = \frac{1}{2\pi}[\ln(x^2 + y^2) + 3.44388] - 0.033425. \tag{4}$$

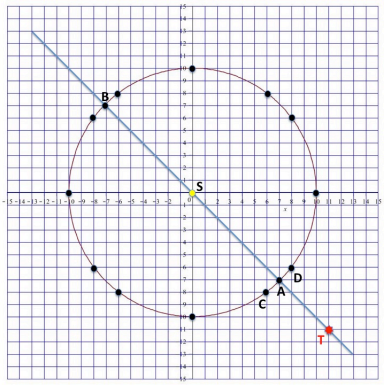


Figure 2. Proposed circle distribution of on-chip sensors.

As can be seen from (4), for a certain power grid with constant r, the effective resistance between any two points is only affected by the Euclidean distance of that two points within the power grid. If on-chip sensors are utilized for real time monitoring of ICs and those sensors are distributed on a circle with the power supply at the center of that circle, R_{sn} will be equal for all sensor nodes on that circle since the Euclidean distance between any sensor on the circle and the power supply point is equal to the radius of the circle.

One example of the circle distribution of sensors with a radius of 10 is shown in Fig. 2. The black dots on the cross points of the circle and the power grid stand for the on-chip voltage sensors and the yellow dot at the center of the circle depicts the on-chip current sensor. Voltage sensors are utilized to measure the instant voltage at a certain power grid node and the current sensor is utilized to judge if the total current change is greater than a certain threshold value. The red point in the figure stands for the location of the Trojan.

Coarse estimation of the Trojan location: Assume at time t_1 and t_2, node voltages measured at C (x_C,y_C) and D (x_D,y_D) are, respectively, (V_{C1},V_{C2}) and (V_{D1},V_{D2}) and Trojan is activated at (x_T, y_T) during this time interval. Node voltage changes at nodes C and D during this time period can be obtained using (2). According to (4), $R_{snC} = R_{snD}$

The error can be defined as

$$err = |\Delta V_D - \Delta V_C| = \tfrac{1}{2} |I_{Trojan} \times (R_{n_D t} - R_{n_C t})|. \tag{5}$$

If during a certain time period, it is observed that

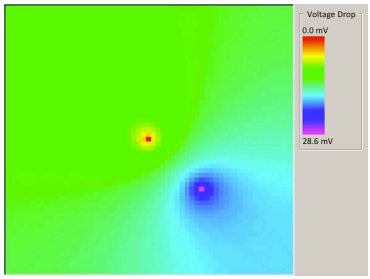
$$\Delta V_C = \Delta V_D \neq 0, \tag{6}$$

then the Trojan is activated and *err* is approximately equal to zero. Since Trojan current is unlikely to be zero, it can be inferred that during this time interval, the activated Trojan location meets the condition $R_{nDt} = R_{nCt}$, which is equivalent to

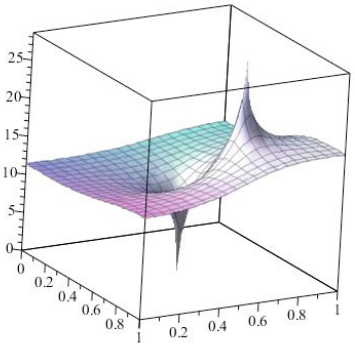
$$(x_D - x_T)^2 + (y_D - y_T)^2 = (x_C - x_T)^2 + (y_C - y_T)^2. \tag{7}$$

The intuitive explanation of (7) is that the Euclidean distance between sensor C and the Trojan, and that between sensor D and the Trojan are equal. Locations meeting the requirement of (7) lie on the perpendicular bisector of line segment CD. By observing the same delta V changes at two different sensor nodes, Trojan location can be defined on a straight line.

Also, by observing (2) and $R_{nDt} = R_{nCt}$, sensor node on the circle which makes the smallest R_{nt} will have the maximum absolute delta V value and sensor node which makes the largest R_{nt} will have the minimum absolute delta V value. The smallest R_{nt} means the shortest Euclidean distance between the sensor node and the Trojan and the largest R_{nt} means the longest Euclidean distance between the sensor node and the Trojan. As shown in Fig. 2, the shortest and the longest Euclidean distances between any sensor nodes on the circle and the Trojan occur at the line segment AT and BT, respectively. Since cross points A and B are on the line defined by ST, by finding the maximum or the minimum absolute delta V



(a) 2D view



(b) 3D view

Figure 3. Map of the voltage fluctuations of a 60 by 60 power grid due to the activation of the Trojan.

among all sensors, Trojan location can be easily defined on the line SA, SB or AB.

Fine estimation of the Trojan location: To estimate the location of the Trojan more accurately, the distance between the power supply and the Trojan needs to be found. Thus, the Euclidean distance between the power supply and the Trojan is defined as *l* and system equations are constructed below to obtain *l*. According to (2), the ratio of two delta V values at sensor nodes A and B is

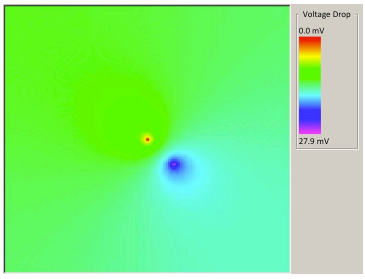
$$\frac{\Delta V_B}{\Delta V_A} = \frac{R_{sn_B} + R_{st} - R_{n_B t}}{R_{sn_A} + R_{st} - R_{n_A t}}. \tag{8}$$

Line segment ST = *l*.
Combined with (3), (8) can be expressed as

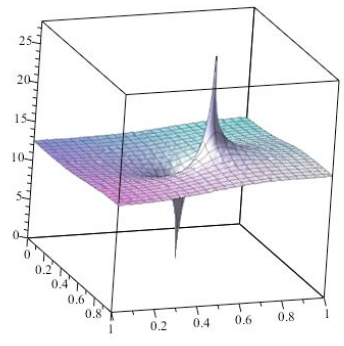
$$\left(\frac{\Delta V_B}{\Delta V_A} - 1\right) \ln(l) - \frac{\Delta V_B}{\Delta V_A} \ln|l - r_C| + \ln(l + r_C) = \left(1 - \frac{\Delta V_B}{\Delta V_A}\right) [\ln(r_C) + 1.61693]. \tag{9}$$

Equation (9) can be solved using numerical analysis to define Trojan locations. After *l* is obtained, Trojan current can be estimated by using

$$I_{Trojan} = -\frac{2\Delta V_A}{R_{sn_A} + R_{st} - R_{n_A t}} = -\frac{2\Delta V_B}{R_{sn_B} + R_{st} - R_{n_B t}}. \tag{10}$$



(a) 2D view



(b) 3D view

Figure 4. Map of the voltage fluctuations of a 120 by 120 power grid due to the activation of the Trojan.

Simulation Results

Power grids with size of 31 by 31, 60 by 60, and 120 by 120 are simulated in Cadence to verify the accuracy of the proposed method. For comparison purposes, all of the simulation conditions except the size of power grid are the same. Power supply voltage of 1 V at location (0,0), load current of 100 mA at location (-3, -12), and Trojan current of 20 mA at location (11, -11) are used for all the simulations. Node voltage changes of 60 by 60, and 120 by 120 power grids in both 2D and 3D view are, respectively, shown in Figs. 3 and 4. It can be seen that the maximum voltage drop happens right at the Trojan activation point and absolute delta V values around Trojan activation point drop quickly. Absolute delta V values far away from Trojan are much lower and quite constant. Thus, it is more accurate to utilize sensors near the maximum voltage change node for comparison. Also, as the size of power grid increases, the maximum absolute delta V value becomes smaller.

The simulated and estimated Trojan location *l*, Trojan current I_{Trojan} and corresponding percentage errors are summarized in Table 1 and Table 2. As the size of power grid increases, percentage error drops rapidly and the proposed circle distribution method becomes more accurate. In fact, the proposed Trojan detection and location method is based on the closed form expression of the effective resistance model and an infinite grid is assumed to determine the effective resistance of a finite

Table 1. Accuracy of the Trojan Location Estimation in Power Grids with Different Sizes

Power grid size	Simulated *l*	Estimated *l*	Percentage error
31 by 31	15.6	11.0	29.5%
60 by 60	15.6	13.8	11.5%
120 by 120	15.6	15.4	1.3%

Table 2. Accuracy of the Trojan Current Estimation in Power Grids with Different Sizes

Power grid size	Simulated I_{Trojan}	Estimated I_{Trojan}	Percentage error
31 by 31	20 mA	18.2 mA	9%
60 by 60	20 mA	19.5 mA	2.5%
120 by 120	20 mA	19.9 mA	0.5%

power grid which leads to approximation error [6][7]. As the size of modern power grids can be very large and typically exceeds 100 by 100 [6][7], the approximation error of the proposed circle distribution method can be negligible. Alternatively, even with a small power grid size and large percentage error, due to the small size of unit power grid and the complex design of hardware Trojan for its malicious functions, the estimated Trojan location can still be sufficient to guide physical inspection of Trojan and be helpful for Trojan isolation or deactivation process.

The resolution of the estimated location of the proposed method can be smaller than the unit size of the on-chip power grid while the on-chip sensor density of the proposed method does not need to be as small as the unit size of the on-chip power grid. As circuit design technology advances, on-chip sensor can become very compact and take less area and resource. A compact multi-use sensor which only uses 8 look up tables (LUTs) is proposed in [8] for on-line sensing for field programmable gate array (FPGA) systems. With compact sensor design and large power grid size, the overhead of the proposed method can be quite negligible. For example, for a circle distribution of radius 10, maximum 32 sensors can be deployed at or near the cross points of circle trace and power grid nodes. The ratio between the maximum number of sensors and the number of nodes of 31 by 31 power grid is around 3.3%. For larger power grid size, the ratio is much smaller, making the addition of security features to critical IC applications less costly.

Conclusions

A hardware Trojan detection and localization approach is proposed in this paper using circle distribution of on-chip voltage and current sensors to implement real-time monitoring of the IC and reduce the number of sensors needed for accurate Trojan location. The procedures for real-time hardware Trojan detection and localization are described and simulation results are provided for three power grids with different sizes. It is shown that with increased size of power grid, the proposed estimation method becomes more accurate. Additionally, even within a small power grid, the proposed method can still be sufficiently accurate to guide the Trojan isolation process. With compact on-chip sensor designs, the overhead of the proposed method can be trivial. The proposed method can be applied to a wide range of hardware Trojan types categorized in [2], including both internally and externally activated Trojans as well as other complex types of Trojans due to the fact that most Trojans incur power change to operate and Trojan activation can lead to node voltage changes. As security concerns arise especially for critical applications, there will be an increasing need for this kind of real-time monitoring scheme for hardware Trojan detection and location using on-chip sensors.

Acknowledgements

This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451, by a Cisco Research Award, and by a seed grant from Florida Center for Cybersecurity.

References

1. S. Mitra, H.-S. P. Wong, and S. Wong, The Trojan-Proof Chip, *IEEE Spectrum Magazine*, Vol. 52, No. 2, pp. 47-51, February 2015.
2. M. Tehranipoor and F. Koushanfar, A Survey of Hardware Trojan Taxonomy and Detection, *IEEE Design and Test of Computers*, Vol. 27, No. 1, pp.10-25, 2010.
3. Y. Jin and D. Sullivan, Real-Time Trust Evaluation in Integrated Circuits, *Proceedings of DATE*, pp. 1-6, March 2014.
4. X.Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis, *IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems*, pp. 87-95, 2008.
5. S. Kelly, X. Zhang, M. Tehranipoor, and A. Ferraiuolo, Detecting Hardware Trojans using On-chip Sensors in an ASIC Design, *Journal of Electronic Testing*, Vol. 31, No. 1, pp. 11-26, 2015.
6. S. Köse and E. G. Friedman, Efficient Algorithm for Fast IR Drop Analysis Exploiting Locality, *Integration, the VLSI Journal*, Vol. 45, No. 2, pp. 149-161, 2012.
7. S. Köse and E. G. Friedman, "Effective Resistance of a Two Layer Mesh," *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 58, No. 11, pp. 739 - 743, November 2011.
8. K. M. Zick and J. P. Hayes, On-Line Sensing for Healthier FPGA Systems, *Proceedings of the ACM/SIGDA International Symposium on Field Programmable Gate Arrays*, pp. 239-248, 2010.