TELKOMNIKA, Vol.16, No.2, April 2018, pp. 573~579
ISSN: 1693-6930, accredited **A** by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v16i2.6812

Detection of Malicious Circuitry Using Transition Probability Based Node Reduction Technique

Nirmala Devi M*, Irene Susan Jacob, Sree Ranjani R, Jayakumar M
Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, Amrita University, India
*Corresponding author, e-mail: m_nirmala@cb.amrita.edu

Abstract

In recent years, serious concerns have been raised against the tampering of integrated circuits due to outsourcing of circuits for fabrication. It has led to the addition of malicious circuitry known as Hardware Trojan. In this paper, a transition probability based node reduction technique for faster and efficient Hardware Trojan (HT) detection has been attempted. In the proposed method, the fact that the least controllable and observable nodes or the nodes with least transition probability are more vulnerable as Trojan sites is taken into consideration. The nodes that have lesser activity than the threshold are the candidate nodes. At each candidate node, segmentation is done for further leakage power analysis to detect the presence of Trojans. Experimental results observed on ISCAS'85 and ISCAS'89 benchmark circuits illustrate that the proposed work can achieve remarkable node reduction upto 78.81% and time reduction upto 58.7%. It was also observed that the circuit activity can be increased by varying the input probability. Hence, for further reduction in the Trojan activation time, the weighted input probability was obtained.

Keywords: *Hardware security, Hardware trojans, Transition probability, Weighted input probability, Segmentation*

1. Introduction

The increase in the complexity of the modern electronics has led to an increase in the involvement of various firms from around the globe in each phase of the electronics supply chain. Outsourcing has increased the integrated circuit vulnerability to various malicious activities and alterations. These modifications termed as *Hardware Trojan(HT)* has raised genuine concerns with respect to conceivable dangers to military frameworks, budgetary foundations, transportation security, and healthcare appliances. HTs when introduced in a system, may affect the life span of the system, change the functionality or system specification, leak confidential information or led to denial of service [1-4].

Detection of such malicious alterations is extremely difficult, due to many reasons. To start with, given the vast number of soft, firm, and hard IP centers utilized as a part of SoCs, and in addition the high multifaceted nature of today's IP blocks, distinguishing a little malignant change is extremely difficult. Second, Trojan circuits, by configuration, are normally initiated under certain conditions, which make them inactive and hard to be recognized utilizing random or functional stimuli. Third, tests used to identify fabricating shortcomings, for example, stuck-at and delay faults can not ensure detection of Trojans [5]. Considering these facts, detection of Trojans utilizing basic investigation would be ineffective.

An efficient method to accelerate the HT detection is the need of the hour and the same has been proposed in this work. The method is based on the generation of weighted input patterns to facilitate the activation of the HTs. Moreover, transition probability analysis node reduction has been attempted in the circuit for faster detection of HTs the fact that the least controllable and observable nodes or the nodes with least transition probability are perfect trigger nodes for adding Trojans. Hence by considering only these nodes, the Trojan detection process can be accelerated with the same efficiency as the case wherein all the nodes are under observation. For weighted input pattern generation, an iterative procedure is followed such that the transition probability at each node should be equal to or greater than the user-defined threshold. The main contributions of this paper can be listed as follows:

Received November 29, 2017; Revised February 18, 2018; Accepted February 28, 2018

a. Generation of weighted input probability set, which reduces Trojan activation time.
b. Efficient and high speed Trojan detection technique by reducing the nodes of observation.
c. Validation of the effectiveness of Transition probability based Node reduction technique through extensive circuit-level simulations and by comparing it to the approach without node reduction.

The rest of this paper is organized as follows. In Section II, briefs about hardware trojans and their basic classification. In Section III, the basic idea of the proposed approach is explained including the weighted input pattern generation algorithm and detection algorithm is discussed in detail in Section IV. Section V shows the simulation results using the proposed method, and finally Section VI concludes this paper.

2. Motivation

Design methodologies can assist Trojan detection by employing various testing techniques. Since an adversary always prefers to use rare internal node conditions to develop a Trojan, an approach that increases the node activity can facilitate in improving Trojan detection coverage. An often used strategy is to exercise all functions with critical patterns, instead of the simulation of thorough set of patterns which can be expensive. However, the definition of crucial patterns usually depends on the designer's heuristics [6]. In this paper, the input stimuli is selected in such a way that it increases the transition probability of all the nodes. By increasing the transition probability, it is expected that in case of presence of Trojan, its activation time will decrease and its effect can be seen during the detection phase. Hence, weighted input probability is generated so as to achieve this condition [7].

For faster and accurate response analysis, observation of internal signals of a circuit becomes necessary. Controllability, observability and transition probability at each node are few methods used for observing internal signals [8]. *Controllability* for a digital circuit is outlined as the problem of setting a selected logic signal to *0* or *1*. *Observability* for a digital circuit is the measure of observing the state of a logic signal [8,9]. The controllability and observability measures are helpful as they quantify the difficulty in setting and observing internal signals of a circuit [10,11]. *Probability* defines the risk of obtaining logic *0* or logic *1* on any node of the given circuit. High probability suggests a high circuit activity at that node. The main advantage of those techniques is that they involve topological analysis, however no test vectors [12]. These are static sort of analysis and that they have linear quality, this technique succeeds if the input test stimuli improves the corresponding node activity. Improving the circuit activity increases the triggering action and hence increases the chances of observing variations at the output. Goldenchip free HT detection was discussed in [13], in which power metric based HT detection and diagnosis is done without referring to any reference chip. This nullifies the effect of process variation and the reduced power measurements.

3. Proposed Work

Hardware Trojan detection relies on a threat model that explains a specific Trojan activity within the circuit. Payload is the circuit stricken by the Trojan and trigger initiates the unwanted change in the circuit activity. The inputs to the trigger is the original nodes with low circuit activity. Therefore, this is the basis of the algorithm formulated. The rarely triggered nodes are targeted and the weighted input probability list is generated which increases the activity at these nodes. Figure 1 gives the brief idea of how Trojan detection is carried out in this work.

3.1. Generation of Weighted Input Probability List

For activation of Trojans, the transition probability at each node should be increased. Transition probability threshold ($TP_{threshold}$) is determined as a tradeoff between speed and efficiency of the detection algorithm. In order to enhance the circuit activity of candidate node *n*, whose value is more than $TP_{threshold}$, the distinction between its signal chance being *1* and *0* needs to be reduced, so as to realize this, the input probability of the first input that encompasses a higher influence on the circuit activity of the candidate node will be increased.

Step 1 : Levelization of the test circuit.
Step 2 : Transition probability calculation at each node.
Step 3 : Determination of minimum transition probability when input probability is 0.5.
Step 4 : Determination of maximum value to which transition probability can be increased hence resulting in weighted input probability list.
Step 5 : Calculation of optimum transition probability which can be used as threshold value.
Step 6 : Acquiring rarely triggered nodes.
Step 7 : Segmentation of the circuit taking radius equal to 1.
Step 8 : Equation formulation and solving based on the leakage power analysis of the segments obtained.

Figure 1. Transition Probability Based Node Reduction Technique

Consider the circuit in Figure 2(a), with 0.5 as the input probability, the transition probability for all the nodes is calculated using the formulae from Table 1. At node o[2], the transition probability obtained is 0.234. To increase this value, the transition probability of the corresponding primary input i.e a[2] is increased to 0.7, which results to 0.249 as the increased transition probability of node o[2].

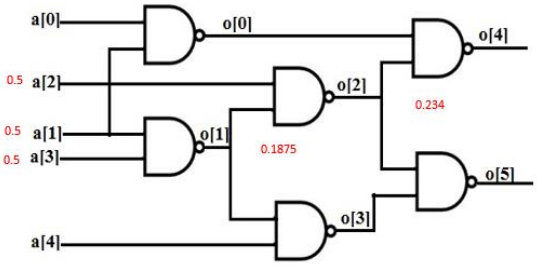

Figure 2(a). c17 ISCAS'85 Benchmark circuit with Initial Transition probability

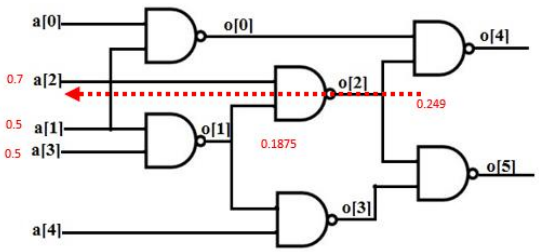

Figure 2(b). c17 ISCAS'85 Benchmark circuit with Reduced Transition probability

Table 1. Formulae for Evaluating Transition Probability of Basic Logic Gates

Logic Gate	Transition Probability ($TP = P_0 \times P_1$)
AND	$(1-P_AP_B) \times (P_AP_B)$
OR	$(1-P_A)(1-P_B) \times (1-(1-P_A)(1-P_B))$
NOT	$(1-P_A) \times P_A$
NAND	$(P_AP_B)(1-P_AP_B)$
NOR	$(1-(1-P_A)(1-P_B)) \times (1-P_A)(1-P_B)$
XOR	$(1-(P_A+P_B-2P_AP_B)) \times (P_A+P_B-2P_AP_B)$

Consider the ISCAS'85 benchmark circuit c1355, it has 41 primary inputs, 32 primary outputs and total number of gates is 546. When the input transition probability is 0.5, the minimum circuit activity is noted as 0.0025. After iteratively increasing the probability list, such that the minimum circuit activity is greater than or equal to the threshold value, it is observed that the minimum circuit activity can be increased to 0.006 without the need of extra hardware. This shows that the circuit activity can be increased upto 63.42%.

Step 1: Computing weighted input probability list such that all the nodes have transition probability greater than $TP_{threshold}$

Input: Netlist of Circuit under test **Output**: List of rarely triggered nodes, weighted input probability list
1. Read the circuit under test and create the input list 2. Divide the circuit into levels to decrease computation complexity 3. Assign input probability as 0.5 for all input nodes 4. Compute transition probability at each node [TP_n] 5. Save the nodes with TP_n less than $TP_{threshold}$ after the first iteration as rarely triggered nodes 6. Check if TP_n is less than $TP_{threshold}$ *if yes :* 7. Increase the input probability of the corresponding input node and repeat steps 4-6 *else :* 8. Prepare the weighted input probability list which will increase the chances of triggering the Trojan.

3.2. Node Reduction Algorithm for Trojan Detection

Step 2: Using the rarely triggered nodes, the presence of Trojan will be detected

Input: Rarely triggered nodes, weighted input probability list **Output**: Trojan detection analysis
1. For all rarely triggered nodes: 2. Divide the circuit into segments such that the gate corresponding to the rarely triggered node acts as the overlapping gate and the number of inputs to this gate determines the number of segments. 3. Remove the segments with primary inputs to the circuit as inputs. 4. Do the leakage power analysis of each segment. 5. Generate the equations using the data obtained. 6. Do the parameter analysis using LP solver. 7. Check if there is a change detected *if yes :* 8. Circuit is Trojan infected *else :* 9. Circuit is Trojan free

In this work, the transition probability at each node is considered for identifying the least controllable and observable nodes i.e. rarely triggered nodes. The rarely triggered nodes come further in use while segmentation is done. Segmentation is implemented around the nodes

identified as rarely triggering nodes in the circuit [14]. Further for Trojan detection, power analysis is considered wherein the presence of Trojan will show a considerable difference in the leakage power.

During segmentation, the rarely triggered node is considered as the centre and then by taking radius as 1, i.e. one logic gate, segments are created and the common gate which has the rarely triggered node as input is considered as the overlapping gate. Figure 3 is used to illustrate the above segmentation procedure wherein the Trojan present at the rarely triggered node will be included in the segment as shown. A change in coefficients is seen in the equations which are formulated based on the input stimuli given to the segment under observation. The coefficients are predetermined as it only depends on the gate and the input given to the gate. The output value of each equation is the overall leakage power of the segment for the corresponding input stimuli. The characterization of a single gate overlapping in multiple segments helps to observe change in variable ouput due to presence of malicious circuitry. In each round of the diagnosis, multiple segments based on number of inputs to the gate with rarely triggered node as the overlapping gate is characterized. Then, the values are tallied for various segments. The one that features a considerable distinction compared to the other values is assumed to be infected [15].

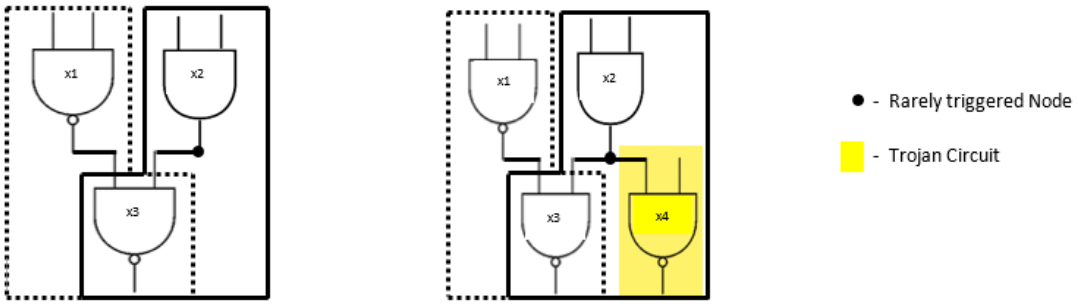

Figure 3. Segmentation Around the Rarely Triggered Node

4. Simulation Results

For various benchmark circuits with different number of controllable nodes, by changing the transitional probability threshold, the rarely triggered nodes are obtained for each case. It is observed that if the threshold is too low then many critical nodes are not considered therefore reducing the system efficiency but the system speed increases whereas if the threshold is very high then nodes under observation increases which increases system efficiency but system speed decreases. Hence, selection of transition probability is a tradeoff between efficiency and speed of the system.

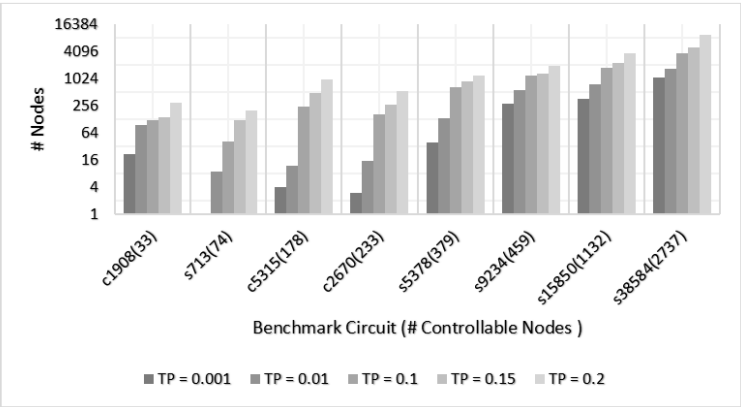

Figure 4. Number of Critical Nodes that Need to be Considered for Varying $TP_{threshold}$

The proposed method aims to detect malicious circuitry at the gate-level wherin the malicious circuitry is added to the netlist by the adversary. In order to validate the proposed methodology, the ISCAS'85 and ISCAS'89 benchmarks are chosen, in which HT attacks based on addition of malicious circuitry is targetted.

Table 1. Transition Probability Based Node Reduction Technique Implemented on ISCAS'85 Benchmark circuit

Circuit	# Inputs	Without Reduction		With Reduction		% Node Reduction	% Time Reduction
		# Nodes	Time (ms)	# Nodes	Time (ms)		
c432	36	153	24.742	42	16.173	72.549	34.633
c499	41	170	21.288	48	13.996	71.764	34.254
c1355	41	514	53.569	112	19.165	78.210	64.224
c1980	33	855	37.517	119	19.491	86.082	48.047
c2670	233	1129	68.059	165	26.597	85.385	60.921
c3540	50	1647	57.449	465	29.021	71.767	49.484
c5315	178	2184	122.865	246	35.488	88.736	71.116
c6288	32	2384	173.861	31	27.485	98.699	84.191
c7552	207	3405	230.432	348	42.982	89.779	81.346
						82.553	58.691

Table 2. Transition Probability Based Node Reduction Technique implemented on ISCAS'89 Benchmark Circuit

Circuit	# Inputs	Without Reduction		With Reduction		% Node Reduction	% Time Reduction
		# Nodes	Time (ms)	# Nodes	Time (ms)		
s298	32	99	38.695	9	16.595	99.909	57.113
s386	20	146	43.766	59	24.269	59.589	44.548
s444	46	154	47.451	25	25.089	83.766	47.126
s526	46	166	50.407	30	29.533	81.928	41.411
s641	73	337	75.173	53	31.205	84.273	58.489
s713	74	351	75.776	41	30.214	88.319	60.127
s838	29	265	66.799	79	34.862	70.189	47.810
s953	52	366	81.411	249	52.691	31.967	35.277
s1488	20	628	111.211	170	47.176	72.929	57.579
s5378	379	2566	202.383	660	69.493	74.279	65.663
s9234	459	5347	446.241	1208	80.376	77.408	81.988
s15850	1132	9102	787.497	1731	107.568	80.982	86.341
s38584	2737	17677	1026.631	3664	364.775	79.272	64.468
						75.062	57.534

5. Conclusion

In this work, a faster and efficient solution of HT detection using node reduction technique is developed. It employs segmentation around the nodes with transition probability less than the user-defined threshold. It was concluded that while selecting the user-defined threshold, the transition probability should be set such that it is neither too high nor too low because high transition probability will increase the number of segments which is again time consuming whereas low transition probability will decrease the efficiency of the system due to the non-consideration of some of the critical nodes. The weighted input pattern obtained was used for faster Trojan activation as it increased the transition probability at each node to a value which is higher than or equal to the user-defined threshold. The proposed method was implemented on ISCAS'85 and ISCAS'89 benchmark circuits and it was observed that it can achieve remarkable node reduction upto *82.55%* and *75.06%* respectively, and time reduction upto *58.69%* and *57.53%* respectively. Hence the proposed technique gives faster and efficient way of Trojan detection.

Acknowledgement

This work is funded by the Defence Research and Development Organization (DRDO), New Delhi, "ERIP/ER/1503187/M/01/1582".

References

[1] M Tehranipoor. Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges. *IEEE Computer Society.* 2011; 44(7): 66-74.
[2] RS Chakraborty. *Hardware Trojan: Threats and Emerging Solutions*. in IEEE International High Level Design Validation and Test Workshop, San Francisco, USA. 2009.
[3] M Abramovici. *Integrated Circuit Security - New Threats and Solutions*. in CSIIR Workshop. 2009.
[4] RS Ranjani, MN Devi. Malicious Hardware Detection and Design for Trust: an Analysis. *Elektrotehniski Vestnik*. 2017: 7-16.
[5] M Tehranipoor. A Survey of Hardware Trojan Taxonomy and Detection. *IEEE Design & Test of Computers.* 2010; 27(1): 10-25.
[6] B Zhou. Cost-efficient Acceleration of Hardware Trojan Detection through Fan-Out Cone Analysis and Weighted Random Pattern Technique. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*. 2016; 35(5): 792-805.
[7] R Chakraborty, S Ranjini, N Devi. A Flexible Online Checking Technique to Enhance Hardware Trojan Horse Detectability by Reliability Analysis. *IEEE Transactions on Emerging Topics in Computing*. 2017; 5: 260-270.
[8] M Bushnell. Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI. New York. Kluwer Academic Publishers. 2006.
[9] H Salmani. COTD: Reference-Free Hardware Trojan Detection and Recovery Based on Controllability and Observability in Gate-Level Netlist. *IEEE Transactions on Information Forensics and Security*. 2016; 12(2): 338- 350.
[10] L Kim. *A Trojan-resistant System-on-chip Bus Architecture*. in Intl. Conf. on Military Communication. 2009.
[11] X Wang. *Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions*. in IEEE Int. Workshop Hardware-Oriented Security Trust (HOST). 2008.
[12] M Potkonjak. *Hardware Trojan horse detection using gate-level characterization*. in IEEE Design Automation Conference. 2009.
[13] RS Ranjani, MN Devi. Golden-chip Free Power Metric based Hardware Trojan Detection and Diagnosis. *Far East Journal of Electronics and Communications.* 2017; 17: 517-530.
[14] H Salmani. *New design strategy for improving hardware Trojan detection and reducing Trojan activation time*. in IEEE International Workshop on Hardware-Oriented Security and Trust, Francisco, CA, USA. 2009.
[15] S Wei. Self-Consistency and Consistency-Based Detection and Diagnosis of Malicious Circuitry. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*. 2014; 22(9): 1845-1853.