Computer Software and Media Applications (2022) Volume 5
doi: 10.24294/csma.v2i1.1172

IP Core Circuit in FPGA Based on Complex Network and Its Security Analysis

Peizheng Yang*
China Jiliang University, Hangzhou 310018, China. E-mail: 523622334@qq.com

ABSTRACT

With the development of technology, IC has entered the era of VLSI. The internal circuit network structure is gradually complex with increasing external threats..Circuit in FPGA can be abstracted into complex network. Then characteristic is studied and the invulnerability is measured to optimize the circuit.

Keywords: FPGA; Complex Network; Invulnerability

In the 1980s, the concept of FPGA was first proposed by Xilinx. As a semi-custom circuit in ASIC further developed on the basis of PAL GAL. The characteristic that FPGA does not need instruction and shared memory gets it high degree of parallelism computing power with low energy consumption. The continuous improvement of performance makes it possible to replace the CPU and GPU in the future. Nowadays, FPGA is widely used. In some important fields, such as communications, its ability to face external threats will determine the extent of the damage. Therefore, the measurement of its destruction resistance will be very important.

1. Overview of FPGA design and IP core circuits

The basic structure of FPGA in hardware generally includes programmable input and output block, configurable logic block, clock management module, embedded RAM block, wiring resources, embedded dedicated hard IP core and low-level internal embedded function unit[1]. One need to familiar with the hardware system and internal resources, and then ensure the code design of the hardware description language to achieve effective cooperation between various components to improve the readability and utilization of the program. This is the main difficulty in FPGA design. The main process to draw feasible FPGA design includes descriptions of the required functions in hardware description language according to user's requirements, such as Verilog, and then usage of software for synthesis, mapping, place and route, verification and testing.

A reasonably designed FPGA has strong advantages over some other devices, so in recent years there has been a trend to use FPGAs to replace other devices. For example, in the field of AI, GPUs are used at the training phase of the DNN models because they provide floating point accuracy and parallel computation, but excessive power consumption cannot be accepted when GPUs are used on edge devices. FPGAs can be reconfigured to implement the latest DNN models and require less power than GPUs[2]. Therefore, in order to obtain suitable FPGAs for different fields, not only must appropriate FPGAs be selected, but it must also be designed reasonably.

Reasonable designs require consideration of constraints such as function, throughput, maximum frequen-cy, area, and power consumption. Throughput, processing speed, and maximum frequency determine performance of devices. It is necessary to design and implement the most required basic functions. Increasing functionality makes applications more versatile but increases area. Maximum frequency depends on the longest path in the design. The pursuit of more throughput and frequency also increases area. Increased

doi: 10.24294/csma.v2i1.1172

area means more power consumption. Power consumption is divided into dynamic power consumption and static power consumption. So it is necessary to get these aspects optimized to obtain the best design.

The required FPGA functions are modularized in order to improve the versatility of the design, avoid repeating the same function modules design to reduce the workload. The IP core is a functional module with specific functions and intellectual property developed by other designers, which provides great support for the modularization. IP cores exist in HDL language form, netlist form and layout form, corresponding to three types: soft IP core, firm IP core and hard IP core. With the development of technology, devices have entered the era of very large-scale integrated circuits. The functions increase, the requirements for device performance become higher and higher, and the designs become more complicated. Through modular design and direct call to the IP cores with corresponding functions in the library, the focus of the designer's work will change from the design of the overall circuit to the design of the architecture, which can avoid repetitive design and reduce the time required to complete complex designs.[3]

2. Characteristics of complex network and measurement of invulnerability

2.1 Characteristics of complex network

The relationship between things is becoming more and more complicated, and it is constructed into various complex networks. Qian Xuesen once gave a definition of a complex network, which is a network with some or all properties such as small world, self-similarity, attractor, and scale-free.

We can effectively analyze various networks by establishing complex network models to simulate real networks. Classic network models include regular network models, random network models, scale-free network models, and some other network models such as the local world evolution network model, etc. Knowing complex networks well requires further analysis of the characteristics of small worlds, clusters, and power laws of complex network. In addition, we can explore the properties of these complex networks such as the degree of nodes $k_i = \sum_{j=1}^{N} (A_{i,j})$, the shortest path $l \equiv < d(v,w) > \equiv \frac{1}{N(N-1)} \sum_{v \in V} \sum_{w \neq v \in V} d(v,w)$, the clustering coefficient $\gamma_v = |\Gamma_v|_g \Big/ \binom{k_v}{2}$, and the eigenvalues of the adjacency matrix[4].

2.2 Invulnerability measures for complex networks

The real network system is abstracted into a complex network of nodes and links, and things are regarded as nodes, and the interrelationship between things is regarded as the network link. As the scale of the actual network becomes larger, the structure of the network becomes more complex, the network is more prone to failure, and the network is more vulnerable to external attacks. Therefore, it is extremely important to measure and analyze the survivability of the network.

The invulnerability of a network describes the ability of a network to resist external damage and restore its function after being damaged. Due to the different definitions and functions of different networks, the definition of indestructibility of networks also varies. It is necessary to analyze the adaptability and reliability of the system to reasonably define the invulnerability of the network according to the positioning of its system and the threats the network may encounter in its operating environment.

The invulnerability measures can be divided into two categories according to the research scope of complex networks: global invulnerability measures and local invulnerability measures. According to the different graph theory models of the networks, it can be divided into: weighted indestructibility measure and non-weighted indestructibility measure.[5] There are also different methods for measuring the invulnerability of complex networks from different perspectives and characteristics of complex networks, including: NCF (Node Connectivity Factor) and LCF (Link Connectivity Factor), LT (Link Tree) and ND (Node Decomposition), Node Degree analysis, maximal connected subgraph, and other link-based measures.[6] For different complex network systems, the selection of a suitable method of invulnerability measurement will become the key to effectively analyze the destruction resistance of the system network.

3. Network characteristics and security of FPGA IP core circuits

3.1 Network characteristics of FPGA circuits

Since the integrated circuit has entered the ULSI era, the rapid development of technology has led to the rapid growth of integrated circuits which has reached the number of billions of transistors integrated in a single chip. For example, Intel's Stratix10 TX FPGA where the number of integrated transistors has reached 30 billion. Its computing capacity has reached 10 trillion times per second, which can provide strong support for 5G network applications such as optical transmission networks and cloud services that require high bandwidth.

Due to the huge number of integrated transistors, the IP core as a node inside the FPGA can form a huge and complex network system. Some changes can be made to the circuit to get the new characteristic parameters of the circuit. By comparing the change of the characteristic parameter and the related characteristics of the circuit, the network characteristics can be studied[7]. Then the theory of the characteristics of complex networks can be used to conduct research to find that the abstract circuit complex networks have Small World Characteristics.

3.2 Invulnerability measurement of FPGA IP core circuits

The invulnerability of FPGA IP core circuit can be defined as the ability of the circuit to tolerate faults and recover normal operations from an attack when exposed to external threats. Holme once proposed that external attacks can be divided into four attack strategies: the initial degrees, the initial betweenness, the recalculated degree, and the recalculated betweenness[8].

When analyzing such a large-scale network of FPGA circuits, we can use a method of local destruction resistance measure proposed by K.T. NewPort: LT and ND.For link j, $LT(j)=\frac{T_j}{T_s}$, Tj is the number of spanning trees containing link j, Ts is the number of spanning trees. For node n, $ND(n)=\sum_{i=1}^{m} c_i^n w_i$, m is the number of different decomposition path lengths k_i. c_i^n This is the probability that node n is included in a path with a decomposition length of k_i. And w_i is the cumulative probability that a path of decomposition length k_i will occur[9]. In this way, the importance of links and nodes can be measured, and calculations can be simplified. This avoids the problem of failing to get good results due to the explosion of calculations when using the global invulnerability measure, NCF and LCF, for complex networks like IP core circuits with very large numbers of nodes. Based on different attack strategies and random attack strategies superimposed to measure the network's invulnerability, the network stability and link stability can be analyzed based on the obtained results.

For some important modules in FPGA, we can use the Node Importance method to evaluate the invulnerability. If a node is in the center, the shortest path between many node pairs in the network must pass through the node. When the node is deleted, the average shortest path length of the network will greatly increase. Network efficiency, $Z=\frac{2}{N(N-1)}\sum_{i=1}^{N-1}\sum_{j=i+1}^{N}\frac{1}{dij}$, is the average of the reciprocal of the shortest path length among all nodes in the network. It represents the ability of information to spread on the network. The degree of nodes v_i is $I_i=1-\frac{Z[G-v_i]}{Z[G]}\times\frac{M-k_i}{M}$. $G-v_i$ is the graph obtained after deleting the node v_i. $M-k_i$ is the number of edges in the graph. After the selected nodes are deleted, the decline in the network efficiency and the number of edges are used as evaluation indexes. These two parameters are the main aspects affecting network connectivity[10].

According to the information obtained by the FPGA IP core circuit's invulnerability measurement and the characteristics of the complex network abstracted from it, we can use the rule-based vulnerabilities scanning, attack graphs, and centralized algorithms based on complex networks to find vulnerable points[11]. Then designers optimize the circuit's security by optimizing the fragile points they find, so as to get a more reliable circuit design.

4. Conclusion

This article summarizes the FPGA IP core large-scale circuit network, discusses the network characteristics, and performs invulnerability analysis through the method of local invulnerability measurement. This article finds out the vulnerable points in the network through the appropriate vulnerability assessment method, optimize them, and then the security of FPGA circuits can be improved.

References

1. Zhao ZQ. FPGA chip design and its application (in Chinese). Electronic Technology & Software Engineering 2018; (21):77.
2. Li ZJ, Zhang YF, Wang J, Lai JM. A survey of FPGA design for AI era (in Chinese). Journal of Semiconductors 2020; 41(2):16-21.
3. Lu CY, Lu DH. Technology and development trend of FPGA. Microelectronic Technology 2003; 31(1): 5-7.
4. Li B. Method for evaluating the damage resistance and node importance of complex networks (in Chinese). Xidian University 2013. doi: 10.7666/d.D364676.
5. Zhang K, Tan GX, Zhuang KC, Zhao RS. Research review on invulnerability mesure of complex network, Computer Era 2010; (05).
6. Newport KT, Varshney PK. Design of survivable communications networks under performance constraints. IEEE Transactions on Reliability 1991; 40(4): 433-440. doi: 10.1109/24.93764.
7. Nie TY, Ma JY, Gao JX. The importance analysis of characteristic parameters in characterizing complex networks of integrated circuits. Information Technology and Information 2019; (1): 98-102. doi: 10. 3969/j. issn. 1672-9528. 2019. 01. 029.
8. Holme P, Kim BJ, Yong CN, Han SK. Attack vulnerability of complex networks. Physical Review E 2002; 65(5): 056109. doi: 10.1103/PhysRevE.65.056109.
9. Newport KT. Incorporating survivability considerations directly into the network design process. Proceedings of IEEE Mil-com 1990; 215-220.
10. Yuan RK, Meng XR, Li MX, Wen XX. Evaluation method for network invulnerability based on node importance. Fire Control & Command Control 2012; 37(10): 40-42. doi: 10.3969/j.issn.1002-0640.2012.10.010.
11. Zhao XL, Xu H, Xue JF, Song TL, Hu JJ, Yan HZ. Research on network system vulnerability detection method based on complex network. Journal of Cyber Security 2019; 4(1): 39-52. doi: 10.19363/J.cnki.cn10-1380/tn.2019.01.04.