Paper ID: 77160
interactive
student

56th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Interactive Presentations - 56th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (IP)

Author: Mr. Kevin Z
University of Electronic Science and Technology of China(UESTC), China

MITIGATING HARDWARE SECURITY RISKS IN SPACE STATIONS: AN INTEGRATED APPROACH FOR BUILDING A SECURE ENVIRONMENT

Abstract

In recent years, the integrated circuit industry has become the fundamental support of the information society and has been widely applied in various fields such as industry, healthcare, military, and aerospace. With the increasing integration and precision of integrated circuits, it has become increasingly difficult for a single manufacturer to complete the entire design process of the circuit. This situation makes it easy for third-party attackers to implant special function hardware Trojans into circuits manufactured by multiple suppliers from different countries. In particular, special-purpose chips used in the aerospace industry are vulnerable to hardware Trojan attacks, which may cause the entire electronic system of the aerospace station to collapse, resulting in incalculable losses. Thus, thorough detection of hardware Trojans is of paramount importance.

In previous studies, feature detection for gate-level circuits has typically focused on wire nodes, which has yielded good results for small-scale circuits. However, with the development of the integrated circuit industry, chip size and design complexity continue to increase, and the detection method that only targets small circuits has become increasingly unsuitable for today's integrated circuits. Another method for detecting hardware Trojans at the netlist level typically involves converting the netlist into a directed graph and using the inherent structure of the hardware Trojan to determine its presence. However, this method is resource-intensive and time-consuming, resulting in low efficiency, and is also difficult to implement for large-scale circuits.

In this paper, we address the aforementioned issue by proposing a hardware Trojan detection method based on physical characteristics of the netlist. By combining netlist physical features with machine learning, we utilize K-nearest neighbors, random forest, and support vector machines to construct machine learning classifiers. We use the SMOTETomek algorithm to address the problem of an imbalanced Trojan feature dataset, thereby detecting hardware Trojans. We modified the publicly available Trojan provided by trust-hub and successfully detected these new Trojans, resolving the issue of incorrect detection when the structure of hardware Trojans changes, which is prevalent in most netlist-level hardware Trojan detection methods. This method ensures both a high detection accuracy and a short detection time while reducing resource usage. Thus, it safeguards the hardware security of space stations and other aerospace systems.