

引用格式: 李鑫, 李海明, 马健. 基于电路结构分析的集成模型检测硬件木马[J]. 微电子学与计算机, 2021, 38(5): 80-86. [LI X, LI H M, MA J. Hardware trojans detection based on circuit structure analysis and integrated model[J]. Microelectronics & Computer, 2021, 38(5): 80-86.]

基于电路结构分析的集成模型检测硬件木马

李 鑫, 李海明, 马 健
(上海电力大学, 上海, 200000)

摘 要: 硬件安全已经成为当今时代备受瞩目的焦点问题, 硬件木马检测的技术也逐渐变得多样化. 针对硬件木马的检测, 本文提出一种基于电路结构分析的集成模型. 该方法利用遍历的方法提取硬件木马三组门级特征, 采用 NLP 思想与方法和 RobustScaler 标准化的预处理, 将复杂繁琐的电路图转化为向量数据格式, 通过极限梯度提升树和长短期记忆神经网络的集成模型来检测硬件木马. 86.5%TPR 和 97.9%TNR 的实验结果, 有效说明本方法的高效性和准确性.

关键词: 硬件木马; 电路结构; NLP; RobustScaler; 集成模型

中图分类号: TN407 **文献标识码:** A **文章编号:** 1000—7180(2021)05—0080—07

Hardware trojans detection based on circuit structure analysis and integrated model

LI Xin, LI Hai-ming, MA Jian

(Shanghai University of Electric Power, Shanghai 200000, China)

Abstract: Hardware security has become the focus of attention in today's era, hardware Trojans detection techniques are also becoming more diverse. For the detection of hardware Trojans, an integrated model based on circuit structure analysis is proposed in this paper. In this method, three groups of gate level features of hardware Trojan were extracted by topological retrieval, and the complex circuit diagram was transformed into vector data format by NLP idea and method and Robust scaler standardized pretreatment. The hardware Trojan was detected by the integrated model of limit gradient lifting tree and long short memory neural network. The experimental results of 86.5% TPR and 97.9% TNR effectively illustrate the efficiency and accuracy of this method.

Key words: hardware trojans; circuit structure; NLP; robust scaler; integrated model

1 引言

随着半导体工艺技术的不断发展, 电路集成度越来越高, 在芯片中植入的硬件木马只有在特定条件下才可以被激活, 其余时间不影响原始的电路功能, 因此硬件木马被检测出来的难度非常大. 硬件木马是一类实体电路, 在原电路中一旦被植入便会长

期存在, 只有通过合理的检测手段对电路进行木马检测才能使风险最小化, 近年来, 关于硬件木马方面的研究越来越多地引起国内外学者的关注, 对硬件木马检测及防范技术的研究已经到了刻不容缓的地步. 有效的硬件木马检测方法以及防范策略对保证芯片安全、稳定电路系统正常运行至关重要.

收稿日期: 2020—08—09; 修回日期: 2020—09—04

基金项目: 国家自然科学基金项目(61772327); 上海市自然科学基金(16ZR1436300); 上海电力大学智能电网中心(A-0009-17-002-05)资助; 上海市科学技术委员会补助金(15110500700)

2 相关工作

集成电路安全是当今时代需要关注的一个焦点问题,而硬件木马检测作为集成电路安全的一部分,也备受全世界安全领域关注.在过去的一段时间内,硬件木马检测的焦点方向放在逻辑测试^[1-2]与旁信号分析^[3-4]两个主要方面.甚至还提出针对安全性问题,建立辅助电路来帮助硬件木马的检测,将电路冗余部分智能地应用到第三方IP核(3PIP)中来对木马电路进行计数的方法^[5],以及增加认证技术信息来防止电路中插入硬件木马^[6].近些年,随着人工智能地崛起,机器学习也成为了处理数据的一大杀器,因此在硬件木马检测的领域内,也兴起了一些基于机器学习的硬件木马检测方法,比如文献[7-8]采用门级网表的特征分析以及分析基于分类的无硬件木马的电路的自动布局识别.文献[9-10]则提出基于异常检测技术来识别网表中的可疑信号,而这些信号可能是木马的一部分.

在本文中,我们将针对硬件木马检测困难度高,检测效果不明显的现象,提出一种基于电路结构分析的集成模型方法来进行硬件木马检测,该方法将门级电路进行结构分解并分析,根据自然语言处理(NLP)的思想,并借助极限梯度提升树(XGBoost)以及长短期记忆神经网络(LSTM)两种优越的分类器集成的方法来对硬件木马进行检测.首先,将利用Trust-HUB^[11]上下载门级基准电路的网表数据,对门级网表进行遍历,通过遍历电路图上的每个顶点和逻辑结构,将局部结构连接信息由电路图转变为一组逻辑结构序列;然后将采集到的逻辑结构序列数据,利用自然语言处理(NLP)中的5-gram方法将数据转化为向量形式,之后利用RobustScaler方法对向量形式的每组数据进行数据预处理;最后将处理后的每组数据,通过极限梯度提升树(XGBoost)和长短期记忆神经网络(LSTM)分类器集成的方法对实现硬件木马检测的目标.

3 硬件木马特征选取

我们在Trust-HUB^[11]上挑选了12组基准电路作为数据,这12组基准电路中既有不包含硬件木马的正常电路又有包含硬件木马的木马电路,将选取三组硬件木马的特征作为分析.

逻辑门结构关系:对于组合电路中的木马电路触发,尽管硬件木马的触发条件非常少,但是与正常电路相比,逻辑门在数量上会有很大增加并且相互

逻辑门连接关系也会存在变差.因此我们将逻辑门结构关系考虑为硬件木马的门级特征之一,并且对不同类型的逻辑门标注为A,B,C,D,...

触发器结构关系:对于顺序电路,电路中的硬件木马电路部分始终很小,因此在顺序电路中触发电平更小且更难被检测.例如硬件木马触发部分存在电平触发器,当CLK信号为高电平时,硬件木马被激活并接受输入信号,并按照输入信号将触发器输出转置成相应的输出,因此我们同样将触发器结构关系考虑为硬件木马的门级特征之一,并相应的将不同类型的触发器标注为a,b,c,d,...

逻辑循环结构关系:一些硬件木马中具有用于激活触发器的顺序电路.这种顺序电路通常使用循环型的触发器.因此我们定义了一种逻辑循环结构,如图1所示,在图中的底部路径中,可以看出很明显出现了逻辑循环结构,逻辑门A和逻辑门B以及触发器构成了一组逻辑循环结构.同样的将这种逻辑循环结构作为硬件木马的门级特征之一.

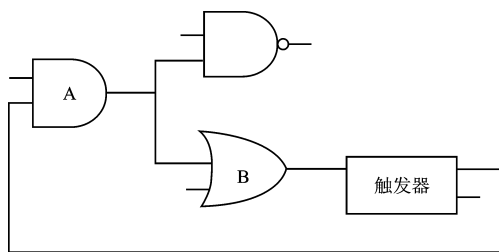


图1 逻辑循环结构

4 特征采集与处理

首先利用遍历方法采集门级网表中电路结构,然后将采集后的电路结构分解,最后利用自然语言处理(NLP)中5-gram的思想,将分解后的电路图结构重新组合生成向量型数据格式,并对数据进行预处理.

4.1 数据采集

利用遍历方法采集门级网表中的电路结构,定义 (V, τ, ω) 的边集 τ 是顶集 V 中元素的有序配对, V 为逻辑结构,包括逻辑门和触发器,并将其定义为顶点, τ 为连接逻辑关系的线,我们称之为边缘.因此顶点之间的“连接”是有方向的.有序对的第一个顶点,也就是电路中作为初始输入流过的第一个逻辑结构处开始,到最后一个顶点,也就是电路中最终输出流经的最后一个逻辑结构处结束.而 ω 定义为次数,指代从一处信号开始在两个逻辑之间所经过的次数,例如逻辑循环结构中, ω 值为 $+\infty$,而不存在

逻辑循环结构的一段电路中,两个逻辑之间的 ω 值就为定值. 我们表示根源为顶点 V_1 , 这是具有随机变量 $V_1, V_2, V_3, \dots, V_i$ 的迭代过程, 用 $w_{v_i}^n$ 表示从顶点 V_i 向之后图步, 迭代过程 $w_{v_i}^1, w_{v_i}^2, w_{v_i}^3, \dots, w_{v_i}^n$. 遍历从相邻顶点到最后一个顶点采取均匀采样, 直到遍历所有情况.

4.2 电路结构分解与重组

在 NLP 字段中, 该单词似乎与出现在其前面的四个单词相关. 同样, 我们认为逻辑结构与它之前的四个逻辑结构有关, 尤其是在硬件木马的电路中. 在文献[12]中提出的门级硬件木马特征在特征维数减少后, 其余 11 个特征中的 7 个在 5 级逻辑结构内.

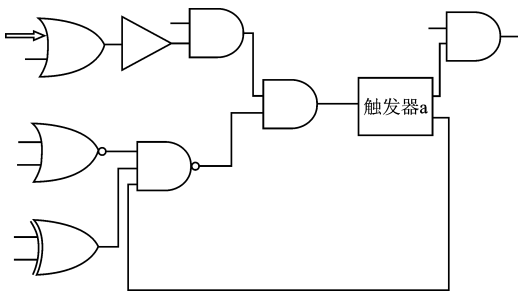


图 2(a) 电路中的一部分结构

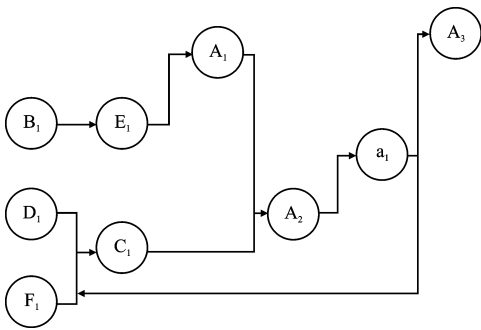


图 2(b) 电路转化为有向图

参考 GramsDet^[13], 使用将传统电路图转换为有向图的想法, 并以有向图的形式表示本文中的三组特征. 图 3 说明了电路分解的过程. 我们将图 2 (a) 一侧的电路结构图转换为图 2(b) 的模式图形式, 并为每个逻辑门和触发器描绘一个不同的字母, 以表示逻辑循环结构, 然后我们为逻辑结构的每一层具体编号, 以便我们可以确定循环结构在电路中的位置, 以确定硬件木马的位置. 这也是我们对 GramsDet^[13] 的改进之一. 特别是, 我们将逻辑循环结构表示为图 3 中的最后一种情况, 这意味着很明显哪些逻辑结构属于逻辑循环结构, 并且简化了其他路径通过逻辑循环结构的过程, 避免了重复和

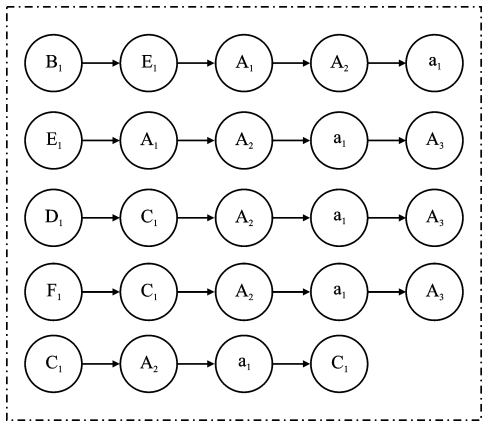


图 3 电路分解与重组

困难.

在自然语言处理(NLP)领域中, 单词共现的统计是描述各个单词是如何一起出现, 进而来捕获单词之间存在的关系. 单词共现统计信息是通过简单地计算两个词在语料库中给定大小的单词窗口中如何同时出现来计算的. 显然, 这种方法是不考虑单词之间的顺序或位置关系. 但是在电路设计中, 逻辑结构之间的不同顺序意味着不同的电路连接结构^[13]. 我们参照 NLP 领域方法, 设计了逻辑结构的顺序共现矩阵 $OC[N] \times [N]$, 该共现矩阵是个满阵, 行向量与列向量数都为 N , 表示各种逻辑结构之和. 让计算 $M(\text{logic_beh}|\text{logic_pre})$ 表示后面的逻辑结构在基准电路库中跟随先前的逻辑结构的次数. 但计算值 M 为 2 时, 就可以统计汇总顺序共现信息, 如表 1 所示.

表 1 电路结构的顺序共现矩阵

OC	A ₁	A ₂	A ₃	B ₁	C ₁	D ₁	E ₁	F ₁	a ₁
A ₁	0	2	0	0	0	0	0	0	0
A ₂	0	0	0	0	0	0	0	0	5
A ₃	0	0	0	0	0	0	0	0	0
B ₁	0	0	0	0	0	0	1	0	0
C ₁	0	3	0	0	0	0	0	0	0
D ₁	0	0	0	0	1	0	0	0	0
E ₁	2	0	0	0	0	0	0	0	0
F ₁	0	0	0	0	1	0	0	0	0
a ₁	0	0	3	0	1	0	0	0	0

在构造的逻辑结构顺序共现矩阵中, 行向量和列向量都具有相关的含义. 行向量表示顺序连接到当前逻辑结构的下一级逻辑结构, 并记录下一级逻辑结构和次数. 列向量表示依次连接到当前逻辑结构的上层逻辑结构, 并记录上层逻辑结构和次数. 特

别是,我们将从同现矩阵中了解到,逻辑回路结构 $C_1 \rightarrow A_2, A_2 \rightarrow a_1, a_1 \rightarrow C_1$ 出现在有向图中,这清楚地表明我们的方法可以代表硬件木马的特征.是逻辑循环结构.最后,我们将逻辑结构的顺序共现矩阵中的列向量和行向量连接起来,以生成向量数据格式.例如, C_1 的向量形式为 $[0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 3, 0, 0, 0, 0, 0, 0, 0]$.

4.3 数据预处理

数据预处理主要包括缺失异常值处理和归一化.如将缺失异常值舍去或取均值填充,可能会忽略某些重要信息或掺入噪声,对检测结果造成不良影响.本文中的处理数据方法可能会出现少量异常值,为了保持门级电路数据的完整性和原始性,我们不直接对数据做异常值处理,而是在数据归一化阶段采用 RobustScaler 标准化方法来针对离群点做处理.

5 XGBoost 与 LSTM 集成模型

5.1 XGBoost

极限梯度提升树(XGBoost)是 Boosting 集成学习的一种算法.基于 XGBoost 算法的检测模型采用 CART 树作为基学习器,输入经预处理的特征数据,通过构建多个弱学习器,逐层迭代学习以最小误差为目标来训练模型,最后通过加权求和得出最终检测结果.如图 4 所示. XGBoost 目标函数的详细推导可参考文献[14].

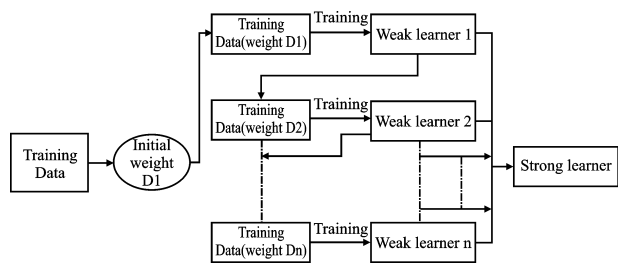


图 4 XGBoost 体系结构

5.2 LSTM

LSTM 网络是通过一种被称为存储块的结构对数据进行丢弃或者添加信息.典型的 LSTM 神经网络包括多个层,包括序列输入层, LSTM 层和回归输出层. LSTM 层的基本单位称为存储块,存储块的内部架构如图 5 所示.

5.3 模型集成方法

我们使用 XGboost 与 LSTM 两种基模型集成的方式组成新的检测模型,新模型采用 stacking 的集成方法将双种模型进行组合,并采取 5 折的交叉

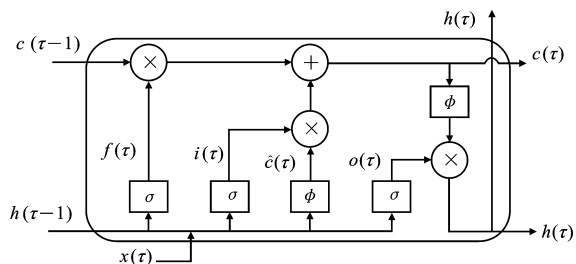


图 5 LSTM 神经网络体系结构

验证方式,来分批训练模型. Stacking 的主要思想是训练模型来学习使用底层学习器的预测结果.如图 6 所示.

5.4 检测流程

设计的检测方法总体流程如图 7 所示,主要为:

(1)特征选择:从 Trust-HUB^[11]上面下载的门级网表数据,利用遍历方法采集门级网表中的电路结构,电路结构中包含文中所提的三种特征.

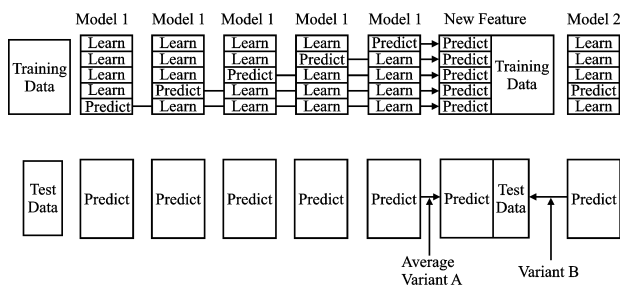


图 6 Stacking 模型集成

(2)数据处理:对原始数据集利用 NLP 领域内的方法对电路结构进行分解与重组,然后进一步选取相关特征数据结构进行数据预处理,处理过程中采用对含有少量异常值,鲁棒性好的 Robust 标准化方法对数据归一化.

(3)集成模型:利用 XGBoost 算法的泛化能力强,检测精度高,以及 LSTM 算法的保留梯度反转信息缩减的优势,将两种算法集成综合在一起,充分利用其优势成最终的集成检测模型.

(4)结果与评价:基于 12 种基准电路数据,经过集成检测模型输出最终检测结果,与其他方法进行比较,并做出结果评估.

6 实验与结果分析

6.1 实验配置

在本节中,我们会根据 Trust-HUB^[11]上不同基准电路来评估我们的集成模型,并与其他两种方法做比较.如表 2 中列出的 12 组门级基准电路及其基本信息.使用 scikit-learn^[15]机器学习库在 Python

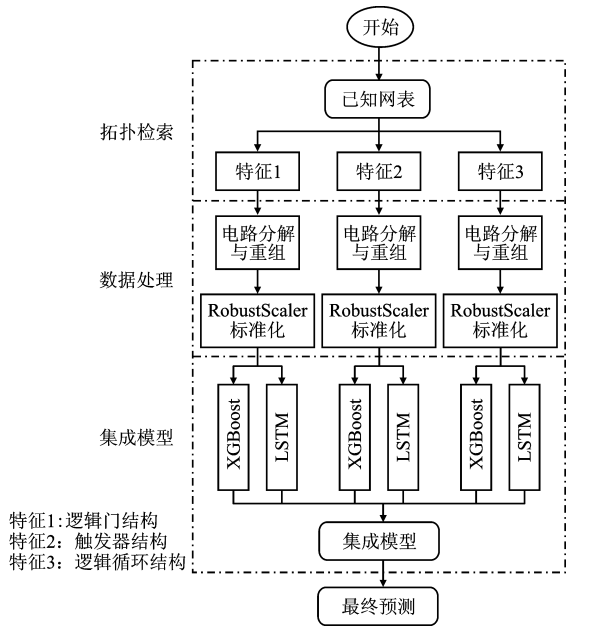


图 7 检测流程图

中的 XGBoost 分类器和 Tensorflow^[16] 平台中的 LSTM 分类器. 我们将表内前 8 组门级基准电路作为训练集, 并将余下的 4 组基准电路作为测试集来评估集成模型效果.

表 2 基准电路和逻辑结构信息

基准电路	正常电路		基准电路	木马电路	
	逻辑结构数量	逻辑结构数量		逻辑结构数量	逻辑结构数量
RS232-T1000	270	36	S38417-T100	5 801	12
RS232-T1100	282	32	S38471-T200	5 803	15
RS232-T1200	280	31	RS232-T1300	284	26
SI5850-T100	2 403	27	RS232-T1400	270	43
S35932-T100	6402	15	S35932-T300	6 403	35
S35932-T200	6 405	12	S38417-T300	5 805	44

由于木马电路中逻辑结构数量相比正常电路中逻辑结构数量较少, 因此, 将正常网络中逻辑结构的总数记为 N_o , 木马电路中逻辑结构的总数记为 N_t , 并复制木马电路中所有训练数据 $[N_o / N_t - 1]$ 次, 以形成与正常电路中逻辑结构数量相似大小的数据, 这样就形成了一个新的平衡数据集用于训练. 同样的, 为了防止数据过拟合, 使用了留一法交叉验证方法^[17] 来验证检测方法的有效性.

6.2 实验与结果

我们使用集成模型来检测电路中可能出现的硬件木马. 本文采用数据分类中的评估指标真实阳性率(TPR)和真阴性率(TNR), 其中 TPR 表示为被集成模型正确检测为木马电路逻辑结构的数量占真

实木马电路中逻辑结构的总数百分比, 而 TNR 则表示为被集成模型正确检测为正常电路逻辑结构的数量占真实正常电路中逻辑结构的总数的百分比. 通过两个评估指标能明确的看到检测实验的结果, 并与其他方法进行比较, 证明本方法的优越性. 实验结果如表 3 所示.

表 3 各基准电路实验结果

基准电路	TPR/%	TNR/%	基准电路	TPR/%	TNR/%
RS232-T1000	100	98.3	S38417-T100	79.9	99.7
RS232-T1100	98.1	99.2	S38471-T200	83.1	100
RS232-T1200	89.2	100	RS232-T1300	98.1	99.4
SI5850-T100	81.1	97.6	RS232-T1400	96.7	97.3
S35932-T100	86.7	96.2	S35932-T300	90.1	99.4
S35932-T200	73.1	97.5	S38417-T300	62.3	90.5

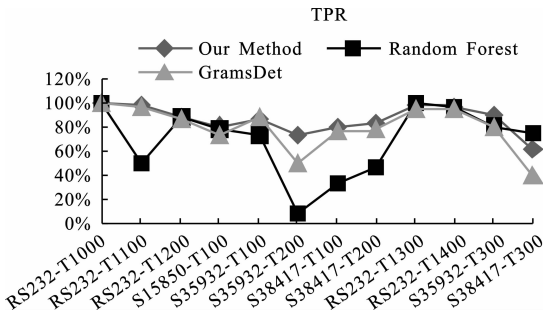
从表 3 内可以看出, 我们的检测模型效果良好. 特别的是在这 12 种基准电路中, 最大值的 TPR 和 TNR 都达到 100%, 这也就意味着无论逻辑结构在正常电路中还是在插入硬件木马的电路中, 我们的检测集成模型都能做出正确的判断. 在所有的基准电路中, TNR 准确率都达到了 90% 以上, 这也说明了我们的检测集成模型对正常电路具有很好的检测效果. 而 TPR 的值在不同的基准电路检测效果就有很大的不同, 例如在 RS232 系列的基准电路中, TPR 的效果还是很好, 基本上在 90% 以上, 这说明在 RS232 系列的组合型集成电路中, 我们所提取的硬件木马特征, 具有突出性和重要性的优势. 但是在其他类型的基准电路, 例如 S35932 系列电路中, 检测集成模型的效果相比 RS232 系列集成电路效果就要相差很多, 原因在于我们所提取的硬件木马特征不够明显, 不具有代表性. 例如 S38417-T100 电路属于时序电路, 而 RS232 系列电路属于组合电路. 针对时序电路中的硬件木马, 我们所提取的硬件木马特征还存在不足. 后续的工作会分析时序电路结构来完善硬件木马特征, 进而提高检测效率.

6.3 实验比较

我们将本文的方法与其他两种方法随机森林^[12]和 GramsDet^[13] 分别在 TPR 和 TNR 两种数据进行比较, 结果如下. 为了展现本方法的优越性, 我们将在两个方面展现比较结果, 首先在每种基准电路的检测上, 如图 8 所示, 我们分别从 TPR 和

TNR 来作比较。

在实验比较中,就 TPR 的角度分析,在所有测试的基准电路中,我们的方法相比另外两种方法的效果更好,曲线更平滑。虽然有小部分基准电路中的结果比另外两种方法差,例如 S35932-T100 和 RS232-T1300,但是在大部分基准电路的结果都比另两种方法的结果明显。从 TNR 的角度分析,我们的方法相比 GramsDet^[13] 还是有部分提升效果。但是就大部分基准电路,我们相比 Random Forest^[12] 还是有不足之处,还有待提高。



(a) 三种方法对于 TPR 值的比较

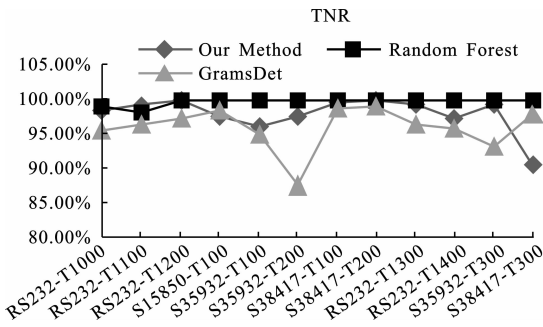


图 8(b)三种方法对于 TNR 值的比较

其次我们在 TPR 和 TNR 在所有测试基准电路的平均值上,与其他两种方法进行了比较。

从表 4 内可以看出,我们的方法比其他两种方法,在 Average-TPR 的角度是有所提高的,硬件木马检测这一研究,主要的目的就是检测正常电路中是否存在硬件木马,因此 TPR 的准确率是非常重要的,更高的 TPR 准确率也就意味着我们的方法能更加高效和精确来检测硬件木马。但是从 Average-TNR 的角度看,我们的方法虽然相比 GramsDet^[13] 是有所提高的,但是相比 Random Forest^[12] 还是有一定的差距。即便检测正常电路不如检测硬件木马电路那么重要,但是就一个模型而言,降低误判率,提高准确率才是最大的提高,未来的工作会在提高 TPR 准确率的同时,兼顾提高 TNR 的准确率。

表 4 三种方法对于平均 TPR 与 TNR 的比较

	本文	Random Forest ^[12]	GramsDet ^[13]
Average-TPR	86.5%	68.3%	80.7%
Average-TNR	97.9%	99.7%	95.5%

7 结束语

在本文中,我们针对硬件木马检测困难的现状,提出了一种基于电路结构分析的集成模型,该模型首先根据自然语言处理(NLP)领域的思想与方法将传统的电路图转化为有向图进行电路分解与重组,然后借助 RobustScaler 标准化的预处理方法提高数据的完整性和精确性,最后在极限梯度提升树(XGBoost)和长短期记忆神经网络(LSTM)算法的基础上创造了检测集成模型。在经过实验检验后,集成模型的检测效果明显,更加有效和准确的检测门级硬件木马,检测结果达到 86.5% 的 Average-TPR 和 97.9% 的 Average-TNR。未来工作将继续放在提高 TPR 的同时兼顾提高 TNR,降低模型误判率,提高准确性。

参考文献:

[1] FLOTTESM L, DUPUISS, BA P S, et al. On the limitations of logic testing for detecting Hardware Trojans Horses[C]//Proceedings of 2015 10th International Conference on Design & Technology of Integrated Systems in Nanoscale Era (DTIS). Napoli, Italy: IEEE, 2015: 1-5. DOI: 10. 1109/DTIS. 2015. 7127362.

[2] WU T F, GANESAN K, HU Y A, et al. TPAD: hardware Trojan prevention and detection for trusted integrated circuits[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2016, 35 (4): 521-534. DOI: 10. 1109/TCAD. 2015. 2474373.

[3] NOWROZ A N, HU K Q, KOUSHANFAR F, et al. Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33 (12): 1792-1805. DOI: 10. 1109/TCAD. 2014. 2354293.

[4] XUE M F, LIU W, HU A Q, et al. Detecting hardware Trojan through time domain constrained estimator based unified subspace technique[J]. IEICE Transactions on Information and Systems, 2014, E97-D(3): 606-609. DOI: 10. 1587/transinf. E97. D. 606.

[5] FARAG M M, EWAIS M A. Smart employment of

- circuit redundancy to effectively counter trojans (SE-CRET) in third-party IP cores [C]//Proceedings of 2014 International Conference on ReConFigurable Computing and FPGAs (ReConFig14), Cancun, Mexico: IEEE, 2014:1-6. DOI: 10.1109/ReConFig.2014.7032562.
- [6] XIAO K, FORTE D, TEHRANIPOOR M. A novel built-in self-authentication technique to prevent inserting hardware Trojans [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2014, 33(12):1778-1791. DOI:10.1109/TCAD.2014.2356453.
- [7] KULKARNI A, PINO Y, MOHSENIN T. Adaptive real-time Trojan detection framework through machine learning [C]//Proceedings of 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, USA: IEEE, 2016:120-123. DOI: 10.1109/HST.2016.7495568.
- [8] NASR A A, ABDULMAGEED M Z. Automatic feature selection of hardware layout: a step toward robust hardware Trojan detection [J]. Journal of Electronic Testing, 2016, 32(3):357-367. DOI: 10.1007/s10836-016-5581-5.
- [9] BAP S, DUPUIS S, FLOTTES M L, et al. Using outliers to detect stealthy hardware Trojan triggering? [C]//Proceedings of 2016 1st IEEE International Verification and Security Workshop (IVSW), SantFeliu de Guixols, Spain: IEEE, 2016. DOI: 10.1109/IVSW.2016.7566609.
- [10] WANG Y Z, HAN T, HAN X X, et al. Ensemble-learning-based hardware Trojans detection method by detecting the trigger nets [C]//Proceedings of 2019 IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan: IEEE, 2019:1-5. DOI: 10.1109/ISCAS.2019.8702539.
- [11] Trust-hub [EB/OL]. [2020-08-02]. <http://www.trust-hub.org>.
- [12] HASEGAWA K, YANAGISAWA M, TOGAWA N. Trojan-feature extraction at gate-level netlists and its application to hardware-Trojan detection using random forest classifier [C]//Proceedings of 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD: IEEE, 2017:1-4. DOI: 10.1109/ISCAS.2017.8050827.
- [13] LU R J, SHEN H H, SU Y, et al. GramsDet: hardware Trojan detection based on recurrent neural network [C]//Proceedings of 2019 IEEE 28th Asian Test Symposium (ATS), Kolkata, India: IEEE, 2019:111-1115. DOI: 10.1109/ATS47505.2019.00021.
- [14] LI S, WANG P, GOEL L. Wind power forecasting using neural network ensembles with feature selection [J]. IEEE Transactions on Sustainable Energy, 2015, 6(4):1447-1456. DOI: 10.1109/TSTE.2015.2441747.
- [15] PEDREGOSA F, VAROQUAUX G, GRAMFORT A, et al. Scikit-learn: machine learning in python [J]. The Journal of Machine Learning Research, 2011, 12:2825-2830.
- [16] ABADI M, BARHAM P, CHEN J M, et al. TensorFlow: a system for large-scale machine learning [C]//Proceedings of the 12th USENIX conference on Operating Systems Design and Implementation, Savannah, USA: USENIX Association, 2016:265-284.
- [17] WONG T T. Performance evaluation of classification algorithms by k-fold and leave-one-out cross validation [J]. Pattern Recognition, 2015, 48(9):2839-2846. DOI: 10.1016/j.patcog.2015.03.009.

作者简介:

李鑫 男, (1994-), 硕士研究生. 研究方向为硬件木马、电路可靠性评估、机器学习. E-mail: 27651625@qq.com.

李海明 男, (1964-), 博士, 教授. 研究方向为智能信号处理的基础和应用研究.

马健 男, (1996-), 硕士研究生. 研究方向为机器学习、电力负荷预测、大数据.