静态软件缺陷预测分析

褚洪波

（黑龙江工业学院电气与信息工程系，黑龙江鸡西，158100）

【摘　要】当前，随着应用软件规模逐渐扩大，软件运行环境也在朝着越来越复杂的方向发展。因此，在应用软件的过程中，必须要提高软件检测结果的可靠性，这样才能更好的解决软件应用中存在的问题。而在当前的软件检测中主要分为动态检测和静态检测两种形式。本文，主要探讨的就是静态软件检测中存在的一些问题，以便能够更好的应用软件检测技术，促使其不断发展和进步。

【关键词】静态软件；缺陷；预测分析

静态检测工具是当前软件检测中常用的一种工具，但是在其具体应用的过程中却经常出现误报、重报和漏报等问题，这些问题的出现影响了软件检测的准确性，对于检测结果也会造成较大的影响。为了更好的发挥静态软件检测的作用。笔者结合自身的工作经验对静态软件缺陷预测进行了详细的分析，希望能借此提高软件检测的实用性和检测的可靠性。

1　静态分析技术概述

所谓的静态分析（Program Static Analysis）是指在不运行代码的方式下，通过词法分析、语法分析、控制流、数据流分析等技术对程序代码进行扫描，验证代码是否满足规范性、安全性、可靠性、可维护性等指标的一种代码分析技术。目前静态分析技术向模拟执行的技术发展以能够发现更多传统意义上动态测试才能发现的缺陷，例如符号执行、抽象解释、值依赖分析等等并采用数学约束求解工具进行路径约减或者可达性分析以减少误报增加效率。目前的静态分析工具，无论从科研角度还是实用性角度还有很大的提高余地，国际最好分析工具误报率在 5-10% 之间，能够报出的缺陷种类也仅有几百种。我国较好静态分析工具较少，一些高校正在致力于在此方面的研究和开发 [1]。

当前市场上的静态检测工具种类极多，而本文在研究过程中主要针对的是 C ++ Test 以及 CBMC 这两种检测工具进行介绍。CBMC 是一个针对 ANSI-C 和 C ++的模型检测器，该检测器比较擅长的是对软件的可靠性进行检测，当软件在应用过程中可靠性存在问题的时候，其能够在较短的时间内感应到。例如对边界缓存溢出、指针安全等方面的检测，该技术的应用就比较灵敏。而且，该检查其还可以对软件程序进行建模验证，并通过建模生成检测报告，对软件缺陷进行分析。

而 C ++ Test 则是针对 C/C ++的一款自动化测试工具，该软件在使用过程中能够较好的提升软件开发团队的工作效率，而且能够有效的保障软件的使用质量。在使用过程中，该软件呢首先会对编码进行规范，然后通过静态分析技术对软件的代码进行检测，通过检测保证代码的正确性，并且通过模拟程序找出软件运行时可能会存在的一些问题，一般该工具主要是用在还没有初始化的内存空指针引用除零内存和资源泄露等方面。该技术的应用，有助于提升静态软件检测的可靠性和准确性 [2]。

2　软件缺陷检测模型的设计原理

在进行软件源代码检测时，能够有效的提高软件自身的质量，避免各种漏洞的产生。但是，在具体的检测过程中，仅仅只是依靠常规的软件检测手是不够的，它只能找出代码中的逻辑错误和程序错误等问题，对于更深层次的问题无法进行有效的解决。因此，在解决更深层次问题的时候，需要设计软件缺陷检测模型，根据所设计的模型，科学合理的解决各种各样的问题。当前，大多数的检测模型是结合多种检测工作的检测结果对软件进行分析和统计，进而找出每一项为缺陷的可能性。在具体的检测过程中，通过使用不同的静态检测对程序源代码进行检测，所获得的检测结果也会有所不同。一般工作人员会将检测结果进行一级或者是二级处理，识别并找出软件中的缺陷项和非缺陷项。

在具体的检测过程中，一级处理程序，主要是利用误报和重报规则对数据进行分类，并将误报项和重报项进行标识。在一级处理程序中，静态检测工具的重报率和误报率有所下降。在软件开发过程中，误报率和重报率下降的主要作用，是其减少了开发人员的工作量。因为，在对软件缺陷进行检测的时候，虽然可以运用静态检测法，但是在检测工作完成之后，软件缺陷的确认工作实际上都是需要人工进行最终确认的，如果在检测工作完成之后，没有进行人工复查，会降低检测的准确性，给相关工作的开展带来较大的麻烦。所以说，在人工确认之前需要使用相应的检测工具将误报项和重报项进行标识，这样有利于后期工作的有序开展。

在静态软件缺陷检测中二级处理程序是一种合并优化处理程序，该程序的主要功能是将不同检测工具获取的数据进行优化，然后按照一定的格式对获取的数据进行合并处理，再对合并的结果进行优化，利用重报规则将合并后的数据中的重复项剔除，最终生成结果报告。在二级处理程序中所使用的重复规则与一级处理中所使用的规则略有不同，一级处理所针对的仅仅只是某一种静态检测工具所获得的结果进行处理，而二级处理中则需要对多个检测工具的结果进行处理和合并。此外，在使用静态软件进行缺陷检测的时候，不同的静态检测工具对于同一字段的值域或者是描述的格式是不相同的，所以二级处理过程中还需要添加一个匹配的功能，这样才能够使字段的值域或者是缺陷描述能够找到对应的检测工具，再根据这种检测工具的重报规则和误报规则进行处理，最终将所有的数据进行合并和优化，得到相应的缺陷检测结果。

在应用静态软件的过程中，我们必须要明确不同检测软件的运行机理各不相同，软件检测的重点也存在有较大的差异，通过不同检测软件的结合使用可以对代码进行多方位、多视角而又全面的检测，这样可以较好的提升检测工作的准确性，能够更好的找到软件所存在的漏洞，降低了检测过程中所出现的误报、重报和漏报机率。

总之，在软件应用过程中，对软件的使用效果进行分析检测是不可避免的。在当前的软件检测中，静态软件检测虽然有一定的缺陷，但是从整体使用情况来看，解决好软件的误报、重报和漏报的问题，这样能够更好的实现静态检测技术的使用价值，能够使软件更好的应用，提高我国软件开发质量。

作者简介：褚洪波，1979 年生，女，研究生，教师。

参考文献

[1] 张志武，荆晓远，吴飞．基于非负稀疏图的协同训练软件缺陷预测 [J]. 计算机技术与发展 .2017,(07):38-42.

[2] 万琳，杨腾翔，刘海宁．缺陷数据的相似性度量方法改进 [J]. 计算机系统应用 .2017,(08):152-156.