doi:10.1631/FITEE.1601491

题目：一种使用静态分析和遗传搜索在 Android 恶意软件检测中搜索最优特征的方法

概要：移动设备制造商在全球范围内快速开发各种 Android 版本。同时，网络罪犯也在实施各种恶意行为，例如跟踪用户活动、窃取个人数据以及实施银行诈骗。由于在日常生活中使用 Android 进行重要通信的人群数量庞大，这些网络罪犯从中获得了巨大非法收益。为此，安全从业者通过静态和动态分析对恶意软件进行识别。静态分析具有整体代码覆盖、低资源消耗和快速处理的优势。然而，静态分析需要最少量的特征才能对恶意软件进行有效分类。因此，我们采用基于遗传算法（GA）的遗传搜索（GS）在 106 个字符串中选择特征。为评估由 GS 确定的最佳特征，我们使用了 5 种机器学习分类器，分别是 Naïve Bayes（NB）、功能树（FT）、J48、随机森林（RF）和多层感知器（MLP）。在这 5 种分类器中，FT 仅使用 6 种特征，获得最高准确度（95％）和最高真正率（TPR）（96.7％）。

关键词：遗传算法；静态分析；Android；恶意软件；机器学习