**پایان‌نامه‌ی کارشناسی ارشد: اعظم سادات مقدم قدیری جلالی، ۱۳۹۸**

## تشخیص بدافزار با رویکرد ترکیب طبقه بندها با روش پلکانی

بدافزارهای اندروید با سرعت زیادی در حال افزایش هستند و به یک تهدید جدی و بالقوه برای کاربران تلفن¬های هوشمندی که از پلتفرم اندروید استفاده می¬کنند تبدیل شده¬اند. آنها به سرعت پیشرفت می¬کنند و حریم خصوصی کاربران و اطلاعات محرمانه¬ی آنها را به خطر می¬اندازند. از این رو نیازمند تکنیک¬های موثر و کارآمد برای شناسایی برنامه¬های مخرب اندروید هستیم. این پایان-نامه راهکاری برای تشخیص بدافزارهای اندروید با استفاده از ترافیک شبکه¬ی برنامه¬های کاربردی اندروید پیشنهاد می دهد.این رویکرد شامل دو مرحله است. اولین گام انتخاب مناسبترین ویژگیهای ترافیکی است که در دسته¬بندی ترافیک ورودی به دو دسته-ی بدافزار و بی¬خطر بیشترین تاثیر را دارند. برای این منظور از الگوریتم مربع¬کای برای انتخاب ویژگیهای موثر استفاده می¬کنیم و ویژگیهایی که بیشترین اهمیت را در دسته¬بندی داشتند گزینش می¬شوند. در گام دوم یک مدل پلکانی جدید برای تشخیص بدافزار اندروید با استفاده از ترکیب دو طبقه¬بند ارائه می¬کنیم. سپس ویژگیهای انتخابی مدل ارزیابی شده و با مدل¬های مشابه مقایسه شدند. نتایج نشان دادند که این ویژگیهای انتخابی می¬توانند مدلی، با کارایی مناسب ایجاد کنند. همچنین ارزیابی مدل در چهار سطح امنیتی بررسی شد و نتایج نشان داد که مدل ما می تواند صحت تشخیص بدافزار را به بیش از 95% برساند و نرخ تشخیص اشتباه بدافزار را به کمتر از 0.03% کاهش دهد.

**کلیدواژه‌ها:** تشخیص بدافزار، یادگیری ماشین، ترافیک شبکه، ترکیب طبقه‌بندها

**شماره‌ی پایان‌نامه:** ۱۲۷۴۱۰۱۵۹۷۱۰۰۱
**تاریخ دفاع:** ۱۳۹۸/۰۴/۱۳
**رشته‌ی تحصیلی:** مهندسی کامپیوتر- نرم‌افزار
**دانشکده:** فنی و مهندسی
**استاد راهنما:** دکتر حسن شاکری
**استاد مشاور:** دکتر یاسر علمی‌سولا

## *M.A. Thesis:*

## Malware Detection using Step by Step Ensemble Classification

Android malware is growing at a fast pace and has become a serious threat to smartphone users who use the Android platform. They are progressing rapidly and endangering the privacy of users and their confidential information. Hence, we need effective and efficient

techniques for identifying Android malware. This thesis proposes a strategy to detect Android malware using Android applications network traffic. This approach consists of two steps. The first step is to select the most appropriate traffic features that have the most impact in categorizing traffic into two types of malware and benign. For this purpose, we use a chi-square algorithm to select the effective features and select the characteristics that matter most in the categorization. In the second step, we present a new step-by-step model for detecting Android malware using Ensemble Classification. Then the selected features of the model were evaluated and compared with similar models. The results showed that these selective features can provide a model with proper performance. The model was also evaluated at four levels of security, and the results showed that our model could increase malware detection accuracy to over 95% and reduce the False Positive rate to less than 0.03%.