سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:
ارائه روشی جهت تشخیص بدافزارهای رایانه ای با استفاده از الگوریتم های یادگیری ماشین

محل انتشار:
چهارمین همایش سراسری علوم و مهندسی دفاعی در سپاه (سال: 1394)

تعداد صفحات اصل مقاله: 11

نویسندگان:
مصطفی عباسی - *دانشجوی دکتری، دانشگاه جامع امام حسین (ع)، دانشکده جنگ الکترونیک و دفاع سایبری*

مجید غیوری - *استادیار، دانشگاه جامع امام حسین (ع)، دانشکده فناوری اطلاعات*

خلاصه مقاله:
مسئله اصلی که در این مقاله موردبررسی قرار می گیرد، تشخیص بدافزارهای رایانه ای با استفاده از بررسی فراخوانی هایسیستمی هست که این فراخوانی ها توسط نرمافزارهای تحلیل ساختار بدافزار و اجرا نمودن آنها در محیط های نظارتی مثلسندباکس استخراج می گردد. علت استفاده از سندباکس استخراج رفتارهای بدافزارهای چندریخت و فشرده شده می باشد که باروش های تحلیل ساختاری قابل احصاء نیستند. برای انتخاب زیرمجموعه ای مناسب از فراخوانی های سیستمی برای دستیابی بهالگویی جهت حداکثر نمودن دقت آموزش دسته بندها، از الگوریتم ژنتیک استفاده شده است که در پایان نتایج حاصل از ارزیابیدسته بندهای مختلف به وسیله مجموعه داده ها، ارائه و باهم مقایسه و بهترین دسته بند معرفی می گردد.

کلمات کلیدی:
تشخیص بدافزار، الگوریتم ژنتیک، کروموزوم، دسته بند، شبکه عصبی RB

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/515659