عنوان مقاله:
ارائه روشی نوین جهت تشخیص بدافزارهای چندریختی با استفاده از الگوریتم های همکاری تکاملی

محل انتشار:
کنفرانس بین المللی پژوهش های کاربردی در فناوری اطلاعات، کامپیوتر ومخابرات (سال: 1394)

تعداد صفحات اصل مقاله: 11

نویسندگان:
محمدرضا قاسمی - *باشگاه پژوهشگران جوان و نخبگان ، واحد شیراز، دانشگاه آزاد اسلامی شیراز، ایران*

مسعود دادگر - *مدرس دانشکده فنی و مهندسی شهید باهنر شیراز*

خلاصه مقاله:
افزایش بدافزارها یک تهدید بسیار جدی برای امنیت سیستم های کامپیوتری به شمار می آید.برنامه های ضد ویروس مبتنی بر امضا قدیمی از تشخیص بدافزارهای چندریختی، دگرگون شده و بهطور کلی بدافزارهای کشف نشده ناتوان هستند به طوری که امروزه کامپیوتر میلیون ها کاربر دراینترنت توسط این گونه بدافزارها آلوده شده است. در این مقاله، برای هر کدام از خانواده هایاصلی که در پایگاه داده وجود دارد، یک کد معنایی ساخته می شود. سپس، بر اساس کد معنایی،گراف وابستگی برنامه رسم می شود. این گراف با استفاده از الگوریتم همکاری تکاملی و برازندگیارائه شده با هر کدام از خانوادهها مقایسه می شود. از آنجایی که تعداد گره هر کدام از گراف هامتفاوت است، ترتیبی اتخاذ شده است که بعد از محاسبه میزان برازندگی، تعداد گره گراف نیز درنظر گرفته شوند. بر اساس میزان برازندگی نهایی و حد آستانه، این فایل به عنوان یکی ازخانواده های بدافزار و یا فایل پاک دسته بندی می شود. از نتایج می توان نتیجه گرفت که روش ارائهشده در این پژوهش می تواند به خوبی بدافزارها را کلاسه بندی کند.

کلمات کلیدی:
بدافزار، کد معنایی، گراف وابستگی، الگوریتم همکاری تکاملی