عنوان مقاله:
تشخیص ویروس های کامپیوتری دگرگون شده با استفاده از مدل مخفی پروفایل مارکوف (PHMM)

محل انتشار:
دومین کنگره بین المللی فن آوری، ارتباطات و دانشICTCK۲۰۱۵ (سال: 1394)

تعداد صفحات اصل مقاله: 9

نویسندگان:
سارا زنگویی مفرد - *کارشناسی ارشد دانشگاه آزاد مشهد*

مجید وفایی جهان - *عضو هیات علمی دانشگاه آزاد مشهد*

فرشته رازقی یدک - *کارشناسی ارشد دانشگاه آزاد مشهد*

خلاصه مقاله:
امروزه کمتر سیستمی وجود دارد که در معرض حمله ویروس های کامپیوتری که با گذشت زمان نسل های زیادی را طیکرده ، نباشد. همانطور که طراحان ویروس ها، موتورهای چند شکلی زیادی را ایجاد کردند اسکنر های ویروس هم دردفاع در مقابل ویروسها قوی تر می شوند. اسکنرهای تجاری ضد ویروس معمولاً بر اساس امضا هستند یعنی الگوهایناشناخته را اسکن می کنند تا مشخص کنند که یک فایل ویروسی است یا نه . برای رهایی از شناسایی با امضا ،طراحان ویروس روشهای مبهم کد گذاری را برای تولید ویروس های کامپیوتری دگرگون شده، به کار گرفته اند. چونظاهر ویروس ها از نسلی به نسلی دیگر تغییر میکند اسکنرهای با امضا نمی توانند همه نمونه های ویروس ها راشناسایی کنند. در این مقاله با استفاده از مدل مخفی پروفایل مارکوف ، سیستمی برای تشخیص و شناسایی ویروس-های دگرگون شده پیشنهاد می گردد. همچنین در این مقاله بررسی می شود، که آیا از این مدل میتوان برای شناساییانواع خانواده ویروسهای دگرگون شده استفاده کرد. آزمایش های سیستم بر روی بدافزارهای تولید شده توسط مولدویروس PS-MPC صورت گرفته است و برای مقایسه از فایل های منبع Cygwin به عنوان فایل های سالم استفاده شده است. نتایج بدست آمده نشان میدهد استفاده از مدل مخفی پروفایل مارکوف کارایی مناسبی دارد.

کلمات کلیدی:
اسکنر ویروس، مدل مخفی مارکوف، مدل مخفی پروفایل مارکوف، نرم افزار مخرب، ویروس