عنوان مقاله:
ارائه یک سیستم تشخیص نفوذ مبتنی بر ماشین یادگیری با استفاده کاهش ابعاد ویژگی

محل انتشار:
دومین کنفرانس بین المللی یافته های نوین علوم و تکنولوژی (سال: 1395)

تعداد صفحات اصل مقاله: 10

نویسندگان:
رضا سروانی - *کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی واحد رفسنجان*

محمد علایی - *دکتری معماری کامپیوتر، عضو هیئت علمی گروه کامپیوتر دانشگاه شهید باهنرکرمان*

خلاصه مقاله:
حمله ها به زیرساخت شبکه درحال حاضر تهدید اصلی برای امنیت شبکه و اطلاعات است. بسیاری از سیستم های تشخیص نفود موجود از تمام 41 ویژگی برای ارزیابی و جستجو نفوذ استفاده می کنند که بعضی از این ویژگی ها اضافی و غیرمرتبط هستند. نقطه ضعف این روش ها، وقت گیر و بدون فرآیند تشخیص و کاهش کارایی سیستم تشخیص نفوذ است. در این پژوهش، هدف ایجاد امنیت و تشخیص نفوذ در شبکه های کامپیوتری با استفاده از تکنیک های کاهش ابعاد ویژگی و مدل مخفی مارکوف است. به طور کلی سیستم های تشخیص نفوذ به دو دسته سیستم های مبتنی بر امضا و سیستم های مبتنی بر ناهنجاری تقسیم می شوند. حمله های صفر روزه به حملاتی گفته می شوند که تاکنون توسط سیستم شناخته نشده اند و سیستم های مبتنی بر امضا توانایی تشخیص این نوع حملات را ندارند. در این مقاله یک سیستم تشخیص نفوذ مبتنی بر ناهنجاری ارائه شده است که از کاهش ابعاد ویژگی استفاده می کند. نتایج آزمایشگاهی نشان می دهد که سیستم پیشنهادی نرخ دقت بالاتر و نرخ مثبت کاذب پایین تری نسبت به الگوریتم های قابل مقایسه دارد.

کلمات کلیدی:
سیستم تشخیص نفوذ، ماشین یادگیری، کاهش ابعاد ویژگی، نرخ مثبت کاذب