عنوان مقاله:
ماشین بردار پشتیبان (SVM) با نرمال ساز در سیستم های کشف نفوذ تشخیص حمله در شبکه (وب، سایبر)

محل انتشار:
همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات (سال: 1393)

تعداد صفحات اصل مقاله: 5

نویسندگان:
میترا گودرزی - *دانشکده فنی مهندسی فناوری اطلاعات، دانشجوی دانشگاه نور طوبی تهران، ایران*

ولی سرلک - *دانشکده فنی مهندسی کامپیوتر، استادیار دانشگاه آزاد اسلامی واحد الیگودرز، ایران*

خلاصه مقاله:
هدف این مقاله توضیح و تشریح مسئله تشخیص حمله در شبکه وب و سایبری است، یکی از مشکلاتی که همیشه در شبکه مطرح بوده بحث اهمیت امنیت آن می باشد. افراد سودجو و خراب کار با اهداف مختلف به شبکه حمل می کنند. یکی از شاخه های مهم در شبکه استخراج الگوهای حمله کاربران و ممانعت از حمله های آتی است. یکی از هیافت هایی که در این زمینه بسیار مورد استفاده قرار گرفته است، یادگیری ماشین است. در این روش ها الگوهای حمله به یک روش آموزش داده می شود و سپس با استفاده از مدل یادگیری شده برای داده های تست از آن استفاده نماییم. یکی از مشکلات در این را متنوع بودن ا لگوهای حمله و حجم زیاد داده های موجود است که آنالیز و کشف الگوها را با مشکل روبرو می کند. در این مقاله از روش ماشین های بردار پشتیبان (SVM) برای حل مشکل استفاده شده است. قبل از انجام عمل آموزش نیز داده ها توسط روش Min-Max نرمالیزه می شود. برای تست روش نیز از مجموعه داده ای معروف KDD99 استفاده شده است و به دقت 99/93% دست یافته است. برای پیاده سازی نیز از زبان MATLAB استفاده شده است. در ضمن با استفاده از عمل نرمال سازی در زمان نیز صرفه جویی شده است.

کلمات کلیدی:
شبکه وب و سایبری، تشخیص حمله، روش min-max،، svm