عنوان مقاله:
ارزیابی مجموعه الگوریتم های یادگیری ماشین جهت تشخیص نفوذ

محل انتشار:
همایش ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران (سال: 1395)

تعداد صفحات اصل مقاله: 7

نویسنده:
محمد اخلاق پور - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد اصفهان (خوراسگان)*

خلاصه مقاله:
محبوبیت استفاده از اینترنت منجر به برخی خطرات ناشی از حملات به شبکه گردیده است. تشخیص نفوذ یک مشکل عمده پژوهشی در امنیت شبکه با هدف شناسایی دسترسی های غیرمعمول و یا حملات به شبکه داخلی می باشد. سیستم های تشخیص نفوذ توسط تکنیک های مختلف به یادگیری ماشین نزدیک هستند. براساس تشخیص ناهنجاری سیستم تشخیص نفوذ، رفتار طبیعی و غیرطبیعی با تجزیه و تحلیل ترافیک شبکه در مجموعه داده های مختلف ارزیابی می شوند. چالش های مشترک برای سیستم تشخیص نفوذ، مقادیر زیادی از پردازش داده، نرخ تشخیص کم و نرخ بالای هشدار کاذب می باشند. در این مقاله به بررسی مطالعات مرتبط در دوره های 2011 تا 2016 با تمرکز توسعه واحد، ترکیب و طبقه بندی پرداخته شده است. مطالعات انجام شده توسط طراحی طبقه بندی مجموعه داده و دیگر تنظیمات تجربی مقایسه شده اند و دستاورد و محدودیت های فعلی در حال توسعه سیستم تشخیص نفوذ توسط یادگیری ماشین مورد بحث قرار گرفته اند و موضوعاتی جهت تحقیقات آینده نیز ارایه شده است.

کلمات کلیدی:
یادگیری ماشین، سیستم تشخیص نفوذ، مثبت کاذب، ترافیک شبکه