

عنوان مقاله:

بهبود سیستم تشخیص نفوذ با استفاده از ادغام روش های یادگیری ماشین

محل انتشار:

دومین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی (سال: 1397)

تعداد صفحات اصل مقاله: 13

نویسنده:

محمدحسن نتاج صلحدار - مربی، دانشکده فنی مهندسی، دانشگاه صنعتی شهدای هوپزه، دشت آزادگان، خوزستان، ایران

خلاصه مقاله:

تشخیص نفوذ یک مکانیسم جدید امنیت شبکه برای تشخیص، محافظت و جلوگیری از دسترسی غیرمجاز به یک ارتباط یا شبکه کامپیوتری است. سیستم های تشخیص نفوذ (IDS) یک نقش حیاتی را در نگه داری یک شبکه امن و ایمن، ایفا می کنند. تشخیص نفوذ مبتنی بر ناهنجاری، گروهی از تکنیک ها را که درصدد دسته بندی ترافیک شبکه به صورت طبیعی یا غیرطبیعی است، شرح می دهد. این مورد معمولا شامل دسته بندی باینری داده های انتخاب شده یا جنبه های دیگر یک سیستم است. موفقیت یک سیستم تشخیص نفوذ به این مساله که این سیستم چگونه موفق به ماکزیمم کردن دقت تشخیص و مینیمم کردن نرخ هشدار خطا میشود، بستگی دارد. در یادگیری ماشین، ترکیبی از دسته بندها، به عنوان دسته بند ترکیبی شناخته می شوند که اغلب بهتر از دسته بندهای فردی عمل می کنند. در حالی که تعداد زیادی روش ترکیبی وجود دارد. با این وجود، پیدا کردن یک پیکربندی ترکیبی مناسب برای مجموعه داده های خاص، کار مشکلی است. در این مقاله سعی داریم سه مدل از سیستم های تشخیص نفوذ را با هم ادغام کنیم، که این مدلها شامل، شبکه عصبی-فازی (ANFIS)، ماشین های بردار پشتیبان (SVM) و k نزدیک ترین همسایه (kNN) میباشند. در این مطالعه تجربی، از مجموعه داده شناخته شده NSLKDD استفاده شده است.

کلمات کلیدی:

امنیت شبکه، ANFIS, SVM, KNN, ادغام, NSLKDD

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/849065>

