

عنوان مقاله:

کاهش ویژگی در سیستم های تشخیص نفوذ با استفاده از الگوریتم های فرا ابتکاری

محل انتشار:

چهارمین کنفرانس مهندسی برق، مهندسی مکانیک، کامپیوتر و علوم مهندسی (سال: 1398)

تعداد صفحات اصل مقاله: 11

نویسندگان:

محمد رستمی - دپارتمان مهندسی برق و کامپیوتر دانشگاه آزاد واحد تبریز

فاطمه محمودلو - دپارتمان مهندسی برق و کامپیوتر، آموزشکده فنی و حرفه ای دختران ارومیه، دانشگاه فنی و حرفه ای استان آذربایجان غربی، ایران

خلاصه مقاله:

امروزه برای ایجاد امنیت کامل در یک سیستم کامپیوتری علاوه بر دیوار آتش و دیگر تجهیزات جلوگیری از نفوذ سیستم های دیگری به نام سیستم های تشخیص نفوذ مورد نیاز می باشند تا بتوانند در صورتی که نفوذ گر از دیواره آتش، آنتی ویروس و دیگر تجهیزات امنیتی عبور کرد و وارد سیستم شد آن را تشخیص داده و چاره ای برای آن بیاندیشد. با توجه به حجم زیاد داده ای که در ترافیک شبکه ای وجود دارد استخراج الگوهای برای رفتارهای نادرست کاربران و پیش بینی رفتارهای آنان کاری زمانبر و دشوار است. در این بین، برخی داده ها، در سیستم های تشخیص نفوذ، مزاحم عمل تشخیص نفوذ هستند. ممکن است بین ویژگیهای مختلف داده ها، ارتباط اشتباهی وجود داشته باشد که مانع از تشخیص درست نفوذ شود. احتمال تکراری بودن این ویژگیها نیز وجود دارد، به این معنی که بعضی ویژگیها از ویژگیهای دیگر قابل استنتاج باشد انتخاب ویژگیهای مناسب، میتواند سرعت دسته بندی و یا خوشه بندی را افزایش دهد. این مقاله به بررسی برخی از پر استفاده ترین الگوریتمهای فرا ابتکاری اخیر به منظور انتخاب ویژگی جهت بهبود سیستمهای تشخیص نفوذ میپردازد. نتایج نشان میدهد، استفاده از الگوریتمهای فرا ابتکاری به منظور انتخاب ویژگی در سیستمهای تشخیص نفوذ منجر به افزایش دقت دسته بندیان سیستمها می شود.

کلمات کلیدی:

سیستم های تشخیص نفوذ، کاهش ویژگی، الگوریتم های فرا ابتکاری

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/998785>

