عنوان مقاله:
مدلی برای تشخیص نفوذ چند کلاسه با استفاده از انتخاب ویژگی سنجاقک و جنگل تصادفی بر روی مجموعه داده CICIDS-۲۰۱۷

محل انتشار:
فصلنامه فناوری اطلاعات و ارتباطات انتظامی, دوره 2, شماره 7 (سال: 1400)

تعداد صفحات اصل مقاله: 21

نویسندگان:
محمود نیائی - *دانشجوی دکتری مدیریت فناوری اطلاعات- دانشکده مدیریت و اقتصاد-دانشگاه آزاد علوم تحقیقات- تهران- ایران*

جعفر تنها - *استادیار دانشکده مهندسی برق و کامپیوتر- دانشگاه تبریز- تبریز - ایران*

غلامرضا شاه محمدی - *دانشیار دانشکده مهندسی برق و کامپیوتر- دانشگاه ایوان کی- سمنان- ایران*

علیرضا پورابراهیمی - *استادیار گروه مدیریت صنعتی- دانشکده مدیریت و حسابداری دانشگاه آزاد اسلامی کرج- کرج- ایران*

خلاصه مقاله:
هم زمان با رشد دانش فناوری اطلاعات و وسعت یافتن کاربردهای آن، توسعه مدلهای جدید امنیتی و تحلیل و طراحی روشهای مناسب برای تشخیص نفوذ در شبکه ها و سیستم ها، اهمیت ویژه ای پیدا کرده است. در این پژوهش، یک مدل برای تشخیص نفوذ با عنوانID۲F مبتنی بر انتخاب ویژگی با استفاده از الگوریتم سنجاقک و دسته بندی جنگل تصادفی بررسی و پیشنهاد شده است. روش پیشنهادی، یک روش چند کلاسه می باشد بعبارت دیگر علاوه بر تشخیص نفوذ، نوع حمله را نیز مشخص می نماید. در این پژوهش از دو مجموعه داده کاملا متفاوت CICIDS-۲۰۱۷ وKDD-CUP۹۹ جهت تحلیل استفاده شده تا صحت عملکرد روش با مجموعه داده های متمایز بررسی گردد. مساله با الگوریتم های مختلف اجرا شده و بهترین الگوریتم بعنوان روش پیشنهادی انتخاب شده است. مقدار صحت در روش پیشنهادی بر روی مجموعه داده CICIDS۲۰۱۷ برابر با ۹۹.۸۳ و برای مجموعه داده KDD-CUP۹۹ مقدار ۹۹.۸۵ بدست آمده است. در ضمن نتایج پژوهش با چندین روش دیگر که توسط محققان قبلی پیشنهاد شده مورد مقایسه قرار گرفته است و این مقایسه نشان می دهد که روش پیشنهادی نسبت به اکثر روش های یادگیری ماشین دارای معیارهای ارزیابی بالاتری بوده و زمان اجرای آن نیز بهتر می باشد.

کلمات کلیدی:
تشخیص نفوذ, انتخاب ویژگی, الگوریتم سنجاقک, داده های نامتوازن, CICIDS۲۰۱۷