عنوان مقاله:
استفاده از الگوریتم کلونی مورچگان و روش یادگیری زوجی جهت طبقه بندی حملات در سیستم های تشخیص نفوذ

محل انتشار:
فصلنامه مهندسی مخابرات جنوب, دوره 9, شماره 35 (سال: 1399)

تعداد صفحات اصل مقاله: 15

نویسندگان:
محمد علی ندومی - *مهندسی کامپیوتر، تحصیلات تکمیلی، دانشگاه آزاد، بوشهر، ایران*

مجید سینا - *دکترا، تحصیلات تکمیلی، دانشگاه آزاد اسلامی، بوشهر، ایران*

خلاصه مقاله:
سیستم های تشخیص نفوذ برای ایجاد امنیت در شبکه های کامپیوتری پیشنهاد شده اند تا در صورتی که نفوذگر از سایر تجهیزات امنیتی عبور کرد، بتواند آن را تشخیص داده و از پیش روی آن جلوگیری کند. یکی از مهمترین چالش‌های این سیستم‌ها، ابعاد بالای داده‌های آن می‌باشد. در این تحقیق برای کاهش ابعاد داده‌ای از یک الگوریتم ژنتیک ساده با طول رشته متغیر استفاده می‌کنیم. در مرحله بعد با توجه به ویژگی‌های انتخاب شده، یک مدل فراابتکاری جهت طبقه‌بندی داده‌ها، با استفاده از الگوریتم مورچه‌ها ارائه می‌دهیم. مدل طبقه‌بندی پیشنهادی سعی در تقسیم‌بندی داده‌ها به دو بخش نمونه‌های هنجیده و ناهنجیده دارد. جهت ارزیابی عملکرد روش پیشنهادی از پایگاه داده NSL-KDD که نسبت به سایر داده‌های تشخیص نفوذ از رکوردهای واقعی‌تری برخورد دار است، استفاده می‌کنیم. نتایج حاصل از آزمایشات، عملکرد بهتر روش پیشنهادی را در مقایسه با سایر روش‌های موجود نشان می‌دهد.

کلمات کلیدی:
انتخاب ویژگی, طبقه بندی, الگوریتم ژنتیک, الگوریتم مورچگان, پایگاه داده NSL-KDD