عنوان مقاله:
الگوریتم تولید محافظ در سیستم های تشخیص نفوذ

محل انتشار:
دومین کنفرانس ملی مهندسی نرم افزار دانشگاه آزاد لاهیجان (سال: 1391)

تعداد صفحات اصل مقاله: 5

نویسندگان:
زهرا صادقی - *دانشگاه گیلان، رشت، ایران*

اسدالله شاه بهرامی - *دانشگاه گیلان، رشت، ایران*

خلاصه مقاله:
یک راه تشخیص نفوذ در شبکه های کامپیوتری به کار گیری سیستم های ایمن مصنوعی است که بدلیل ویژگی هایی هم چون وفق پذیری و خود یادگیری مورد توجه محققان بسیاری قرار گرفته است. یکی از اصلی ترین الگوریتم ها دراین زمینه، الگوریتم انتخاب معکوس می باشد. این الگوریتم، مجموعه ای از محافظ ها را برای مقایسه جهت تمایز الگوهای خودی از الگوهای غیر خودی سیستم تولید کرده و به کار می برد. در چنین حالتی، نمونه های مورد آزمایشبرای تشخیص نفوذ نیاز به مقایسه با تمامی محافظ های تولید شده دارند؛ در نتیجه با افزایش تعداد محافظ ها سرعت تشخیص نفوذ نیز کاهش می یابد. بادسته بندی محافظ های نزدیک به هم در یک محدوده مشخص، نمونه های مورد آزمایش که در چنین محدوده ای قرار می گیرند فقط ملزم به مقایسه با محافظ های موجود در همین محدوده می باشند و بنابراین زمان مقایسه کاهش و سرعتتشخیص افزایش خواهد یافت. در این مقاله با انجام دسته بندی بر روی محافظها و تعیین شعاع مناسب برای هر دسته به کاهش تعداد محافظ های قابلمقایسه می پردازیم. با توجه به آزمایشات انجام شده ثابت می شود که دسته بندی محافظ ها به افزایش سرعت تشخیص که عاملی حیاتی در سیستم های تشخیص نفوذ است، منجر می شود

کلمات کلیدی:
سیستم تشخیص نفوذ، سیستم ایمن مصنوعی، الگوریتم انتخاب معکوس،الگوریتم تولید محافظ