پایان‌نامه‌ی کارشناسی ارشد: فرشته سادات ملایی، ۱۳۹۷

ترکیب ماشین بردار پشتیبان با الگوریتم بهینه سازی ازدحام ذرات برای تشخیص نفوذ

در این مقاله، ما چهارچوب تشخیص¬نفوذ را با استفاده از یک روش جدید مطرح می‌کنیم. از ترکیب الگوریتم بهینه‌سازی ازدحام ذرات باینری و پیوسته به ترتیب برای انتخاب ویژگی و بهینه‌سازی پارامترهای ماشین بردار پشتیبان به صورت همزمان استفاده می‌کنیم. الگوریتم ماشین¬های بردار پشتیبان یک الگوریتم قدرتمند برای دسته¬بندی داده¬ها است عملکرد ماشین بردار پشتیبان بستگی به پارامترهای مختلف از قبیل ضریب تخطی C و پارامترهسته ? دارد. همچنین انتخاب یک تابع هسته مناسب می‌تواند میزان تشخیص را بهبود بخشد. علاوه¬ براین، انتخاب وی‌ژگی مفید در میان چندین ویژگی در مجموعه داده‌ها نه تنها عملکرد SVM را افزایش می‌دهد، بلکه زمان و پیچیدگی محاسبات را کاهش می‌دهد. بنابراین این یک مسئله بهینه سازی است که می¬توان توسط الگوریتم¬های اکتشافی حل شود.
در این مقاله ماشین بردار پشتیبان چند کلاسه با روش اعتبار سنجی k_fold به عنوان سیستم کلاسبندی استفاده می¬شود عملکرد روش پیشنهادی با انجام آزمایشات با مجموعه داده NSL_KDD مورد ارزیابی قرار گرفته است و نتایج تجربی نشان می‌دهد که روش پیشنهادی در مقایسه با روش¬های دیگر از لحاظ نرخ تشخیص و زنگ هشدار نادرست بهتر عمل می‌کند.

کلیدواژه‌ها: تشخیص نفوذ بهینه سازی ازدحام ذرات ماشین بردار پشتیبان اعتبارسنجی متقابل انتخاب ویژگی

شماره‌ی پایان‌نامه: ۱۲۷۴۱۰۰۶۹۶۱۰۰۳
تاریخ دفاع: ۱۳۹۷/۰۲/۰۵
رشته‌ی تحصیلی: مهندسی کامپیوتر- نرم‌افزار
دانشکده: فنی و مهندسی
استاد راهنما: مهندس حسام حسن‌پور
استاد مشاور: مهندس علی‌اکبر نقابی

M.A. Thesis:

Combination of Support vector machine with particle optimization algorithm for intrusion detection system

In this paper, the framework of the intrusion detection by the use of a new method is proposed. The combination of the binary and connected particles swarm optimization (PSO) algorithm is respectively and synchronously used for the feature selection and the

parameters optimization of the support vector machine. The support vector machine is a powerful algorithm for data classification, which its function depends on a variety of parameters such as violation factor c and kernel parameter ?. The selection of an appropriate kernel function can also improve the detection rate. Moreover, the selection of the useful feature among a variety of features in data set not only increases SVM function but also decreases time and intricacy in calculation. Therefore, its an optimization issue which can be solved by the exploratory algorithms.
In this article, the multi-class support vector machine is used with the cross validation k-fold method as a classification system. The function of the proposed method has been evaluated by testing the NSL_KDD data set, and the empirical results demonstrate that the proposed method in comparison with other methods operates better in detection and false alarm rate.