چهارمین کنفرانس بین المللی
مطالعات نوین در علوم کامپیوتر و فناوری اطلاعات
4th International Conference
On New studies Of Computer And IT
مشهد
۰۵ اسفند ماه ۱۳۹۶
FEBRUARY 24,2018

ارائه یک سیستم تشخیص نفوذ بهبودیافته با استفاده از خوشه‌بندی گراف و الگوریتم ژنتیک

امیررضا رضوانی ، مهدی ملامطلبی*
گروه کامپیوتر، واحد بوئین زهرا، دانشگاه آزاد اسلامی، بوئین زهرا، ایران

چکیده

یکی از روش‌ها برای برقراری امنیت شبکه، استفاده از سیستم‌های تشخیص نفوذ می‌باشد. این سیستم‌ها با نظارت کردن بر شبکه به‌منظور کشف فعالیت‌های مخرب یا نقض سیاست‌های امنیتی، گزارش‌های مربوطه را برای بخش مدیریت ارسال می‌کنند. یکی از مشکلات پیاده‌سازی سیستم‌های تشخیص نفوذ، زیاد بودن اطلاعات و بالا بودن تعداد ویژگی‌های هر حمله است. درنتیجه، عملکرد سیستم تشخیص نفوذ به‌طور چشم‌گیری پایین می‌آید. مجموعه‌های داده‌ای با ابعاد بالا از دو جهت باعث کاهش عملکرد سیستم تشخیص نفوذ می‌شوند. ازیک‌طرف، با افزایش ابعاد داده‌ها، حجم محاسبات افزایش پیدا می‌کند و از طرف دیگر، مدلی که بر اساس داده‌های با ابعاد بالا ساخته می‌شود دارای قابلیت تعمیم پایینی است. یک راهکار عمده برای مقابله با این مشکل، کاهش ابعاد مسئله از طریق انتخاب ویژگی است. با کاهش ابعاد مسئله، هم پیچیدگی محاسباتی سیستم تشخیص نفوذ کمتر می‌شود و هم عملکرد الگوریتم تشخیص نفوذ ازنظر دقت تشخیص بهبود می‌یابد. در این مقاله، برای انتخاب ویژگی‌های مناسب، یک روش مبتنی‌بر خوشه‌بندی گراف ارائه‌شده است. در این روش، ویژگی‌های اولیه به تعدادی خوشه تقسیم‌بندی شده و سپس از هر خوشه و با استفاده از تکنیک‌های جستجوی تکاملی، ویژگی‌های مناسب انتخاب می‌شوند. روش پیشنهادی با مجموعه داده‌های KDDCUP99 مورد آزمون قرار گرفت. نتایج شبیه‌سازی و مقایسه‌شان با روش‌های مشابه و اخیر، بیانگر عملکرد مناسب روش پیشنهادی در تشخیص نفوذ ازنظر دقت تشخیص نفوذ و کاهش پیچیدگی محاسباتی بوده است.

کلمات کلیدی:سیستم تشخیص نفوذ،الگوریتم ژنتیک، خوشه‌بندی گراف، دقت تشخیص، پیچیدگی محاسباتی