مؤسسه آموزش عالی غیر انتفاعی و غیر دولتی مهرآستان

پایان‌نامه دوره کارشناسی ارشد مهندسی نرم افزار

عنوان:

بهبود تشخیص حملات در شبکه‌های کامپیوتری با استفاده از الگوریتم ترکیبی انتخاب ویژگی

سحر غلام زاده جورشری

استاد راهنما

غلامحسین اکباتانی فرد

شهریور ۱۳۹۴

چکیده

یک سیستم تشخیص نفوذ را می‌توان مجموعه‌ای از ابزارها، روش‌ها و مدارکی در نظر گرفت که به شناسایی، تعیین و گزارش فعالیت‌های غیرمجاز یا تأیید نشده تحت شبکه، کمک می‌کند (Senthilnayaki , 2013). اما در حقیقت سیستم‌های تشخیص نفوذ به‌صورت مستقیم نفوذ را تشخیص نمی‌دهند. درواقع این سیستم‌ها با بررسی فعالیت‌های در حال انجام در شبکه، به کمک الگوریتم‌ها و یا الگوهایی که در خود دارند فعالیت‌های مشکوک را شناسایی کرده و به‌عنوان نفوذ معرفی می‌کنند. طبیعی است که امکان دارد بعضی از این فعالیت‌ها درواقع نفوذ نبوده و صرفاً فعالیتی غیرعادی اما بی‌خطر باشند و سیستم در تشخیص نفوذ دچار اشتباه شده باشد. ابزارهای امنیتی دیجیتال را می‌توان به گونه‌ای معادل ابزارهای امنیتی فیزیکی دانست. سیستم‌های تشخیص نفوذ برای کمک به مدیران امنیتی سیستم در جهت کشف نفوذ و حمله به کار گرفته شده‌اند(Catherine ,2014). هدف یک سیستم تشخیص نفوذ جلوگیری از حمله نیست و تنها کشف و احتمال شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه کامپیوتری و اعلام آن به مدیر سیستم است(Xue-qin , 2006). عموماً سیستم‌های تشخیص نفوذ در کنار دیواره‌های آتش و به‌صورت مکمل امنیتی برای آن‌ها مورد استفاده قرار می‌گیرند. در این پژوهش، قصد داریم با استفاده از تکنیک داده‌کاوی در اطلاعات مربوط به شبکه، حملات احتمالی را تشخیص و دسته‌بندی نماییم. الگوریتم پیشنهادی برای مسأله‌ی انتخاب ویژگی از ترکیب دو الگوریتم ژنتیک و ازدحام ذرات تشکیل خواهد شد.

کلمات کلیدی: انتخاب ویژگی، حملات کامپیوتری، الگوریتم ژنتیک، الگوریتم ازدحام ذرات