الگوریتمی پیشنهادی جهت تشخیص نفوذ در شبکه های کامپیوتری با استفاده از ترکیب روش ازدحام ذرات و طبقه بندی مدل بیزین

حسین حیدری[۱]

[۱] دانشگاه آزاد اسلامی علوم و تحقیقات واحد بوشهر، hheidary@outlook.com

چکیده

امروزه با گسترش روزافزون اینترنت و درنتیجه سیستم های کامپیوتری مبتنی بر شبکه و نقش مهم آنها در ارتباطات و انتقال اطلاعات، شبکه‌های کامپیوتری، نقشی اساسی و فزاینده‌ای در جوامع مدرن ایفا می‌کنند. از اینرو، تامین امنیت این شبکه‌های کامپیوتری، به عنوان یک ضرورت و چالش اساسی برای مدیران امنیتی شبکه‌ها مطرح بوده است. سیستم‌های تشخیص نفوذ، یکی از زمینه‌های مهم تحقیقاتی در امنیت شبکه‌های کامپیوتری هستند. هدف سیستم تشخیص نفوذ، کشف و شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه‌های کامپیوتری و اعلام آن به مدیران امنیتی می‌باشد. از موانع و مشکلات موجود در طراحی یک سیستم تشخیص نفوذ کارامد، می‌توان به حجم انبوهی از داده های مربوط به ترافیک شبکه کامپیوتری، نرخ تشخیص درست پایین و تولید هشدارهای اشتباه، که موجب ایجاد سیستم‌های بسیار بدبین و درنهایت بی‌اعتنایی متخصصان به هشدارهای سیستم خواهد شد، اشاره کرد. در این مقاله با استفاده از ترکیب روش ازدحام ذرات و طبقه بندی مدل بیزین یک روش جدید کشف‌نفوذ ارائه می شود که قادر با شد ضمن تشخیص تعداد بیشتری از کلاس‌های حملات، نرخ تشخیص درست را بهبود داده و همزمان تعداد هشدارهای اشتباه را به حداقل برساند. برای ارزیابی روش پیشنهادی از مجموعه‌داده KDD رایج‌ترین و بزرگ‌ترین مجموعه‌داده استاندارد برای ارزیابی سیستم‌های تشخیص نفوذ، استفاده شد. نتایج نشان داد که روش پیشنهادی از ۲۲ کلاس حمله موجود، ۲۱ کلاس حمله را شناسایی کند و نرخ تشخیص درست به طور میانگین ۹۹ در صد بدست آمد که در مقایسه با روش های مشابه نتایج قابل قبولی داشته است.

واژه های کلیدی

تشخیص نفوذ، بهینه سازی ازدحام ذرات، طبقه بندی مدل بیزین، KDD

مقدمه

امروزه شبکه‌های کامپیوتری نقشی اساسی و فزاینده‌ای در جوامع مدرن ایفا می‌کنند. با گسترش روزافزون اینترنت ودرنتیجه سیستم های کامپیوتری مبتنی بر شبکه و نقش مهم آنها در ارتباطات و انتقال اطلاعات، امنیت این سیستم‌ها همچنان به عنوان یک چالش اساسی برای مدیران امنیتی شبکه مطرح است. سیستم‌های تشخیص نفوذ(Intrusion Detection System) ، یکی از زمینه‌های مهم تحقیقاتی در امنیت شبکه‌های کامپیوتری هستند. وظیفه اصلی یک سیستم تشخیص نفوذ، نظارت بر رویدادهای شبکه کامپیوتری و تجزیه و تحلیل آنها جهت شناسایی و تشخیص اقداماتی است که قصد نفوذ و یا عبور از مکانیزم‌های امنیتی سیستم را دارند.

سازمان ها و ادارات، برای حفظ اطلاعات خود باید از سیستم های امنیتی خاصی استفاده کنند. درنتیجه باید از یک سیاستگذاری و شیوه امنیتی مناسب بهره برند. افزایش کاربرد باعث مطرح شدن مسئله های امنیتی در زمینه ارسال ودریافت اطلاعات شده است؛ در نتیجه امنیت به عنوان مهمترین مسئله مطرح شده است. ازاینرو سیستم تشخیص نفوذ با بکارگیری مجموعه ای از ابزارها، روش ها و مدارک به شناسایی،تعیین و گزارش فعالیت های غیرمجاز یاتائید نشده تحت شبکه می پردازد. سیستم ها، هشداری به مدیر جهت نفوذ رخ داده ارسال می کنند. در این پژوهش نیز از حملاتKDD استفاده شده است همچنین به تاثیر الگوریتم بهینه سازی ازدحام ذرات در شبکه جهت تشخیص هشدارهای مثبت و منفی نادرست، پرداخته خواهد شد .

به دلیل پیچیده‌شدن همواره سیستم‌های کامپیوتری و نقاط ضعف در طراحی و خطاهای برنامه‌نویسی، از نظر تکنیکی ایجاد یک سیستم کامپیوتری فاقد نقطه ضعف و شکست امنیتی، عملا غیرممکن به نظر می‌رسد[1]. بنابراین تامین امنیت شبکه‌های کامپیوتری یک اولویت کاری بالا برای مدیران ارشد و متخصصین امنیتی شبکه‌های کامپیوتری می‌باشد. برای تامین امنیت شبکه‌های کامپیوتری بسته به اهمیت و وضعیت سیستم‌ها، تکنیک‌ها و راهکارهای متنوعی تو سط متخصصین امنیتی، بکار گرفته می‌شود. از جمله دیواره‌ی‌آتش، رمزنگاری، تایید هویت کاربران، امضاهای دیجیتالی و غیره. اما متاسفانه این راهکارها برای تامین امنیت کامل سیستم‌های کامپیوتری کافی نمی‌باشند. بنابراین نیاز به یک مکانیزم امنیتی داریم که پیوسته نظارت کافی بر سیستم داشته، موارد مشکوک به نقض امنیت سیستم را تشخیص داده و پاسخ مناسبی صادر کند. این مکانیزم امنیتی همان سیستم تشخیص نفوذ است. هدف سیستم تشخیص نفوذ کشف و شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه‌های کامپیوتری و اعلام آن به مدیران امنیتی سیستم می‌باشد[2].