عنوان مقاله:
بهبود دقت در سیستم تشخیص نفوذ با استفاده از ترکیب طبقه بندها

محل انتشار:
چهارمین کنفرانس بین المللی مطالعات نوین در علوم کامپیوتر و فناوری اطلاعات (سال: 1396)

تعداد صفحات اصل مقاله: 20

نویسندگان:
سیدعادل نسب الحسینی - *دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد، ایران*

جواد حمیدزاده - *استادیار، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد، ایران*

خلاصه مقاله:
در دنیای امروز، کامپیوتر و شبکه های کامپیوتری متصل به اینترنت نقش عمده ای در ارتباطات وانتقال اطلاعات ایفا می کنند. در این بین عده ای با دسترسی غیرمجاز به اطلاعات مهم مراکز خاص یاافراد دیگر و با مقاصد مختلف، عمل تجاوز به رایانه ها را درپیش گرفته اند. بنابراین محافظت ازاطلاعات و داشتن سیستم کارا برای جلوگیری و تشخیص نفوذ در شبکه های رایانه ای امری اجتناب-ناپذیر است. از آنجا که از نظر فنی ایجاد سیستم ها و شبکه های رایانه ای بدون نقطه ضعف و شکستامنیتی عملا غیرممکن است، از این رو ابزارهای مختلفی جهت شناسایی، هشدار، حفاظت و جلوگیریارایه شده است. سیستم های تشخیص نفوذ ، ضدبدافزارها و دیوارهای آتش نمونه ای از این تجهیزاتهستند. سیستم های تشخیص نفوذ در خط اول دفاعی در مقابل حملات احتمالی قرار دارند. نظر بهپیشرفت فناوری های اینترنتی، نرم افزارها و پروتکل ها، تحلیل ترافیک شبکه بسیار سختتر از گذشتهشده است. سیستم تشخیص نفوذ با بررسی ترافیک شبکه وظیفه شناسایی و تشخیص هرگونه استفادهغیرمجاز از منابع و داده های شبکه را دارد. در این سیستم ها از روشهای متعددی از جمله الگوریتم هاییادگیری ماشین، داده کاوی، الگوریتم ژنتیک، منطق فازی و غیره بهره گیری میشود که هر کدام بهنوعی در تشخیص برخی از حملات نسبت به سایر الگوریتم ها قویتر عمل می کنند. در طول چند سالگذشته سیستم های IDS پیشرفت ها و مطالعات بیشتری را با هدف تشخیص حملات و بهبود بخشیدن به کارایی سیستم و افزایش صحت و دقت تشخیص داشته اند. رویکردهای مختلفی به منظور بهبودالگوریتم ها در فرآیند تشخیص نفوذ ارایه شده است که می توان از جمله کاهش هشدارهای غلط،کاهش ابعاد، کاهش نمونه ها، روشهای ترکیبی، بهسازی مجموعه داده های آموزش و آزمون،بکارگیری روشهای چندسطحی و غیره نام برد. در روش ارایه شده پیشنهادی پساز کاهشویژگیهای موجود در مجموعهداده NSL-KDD از روش گروهی یا به عبارت بهتر ترکیب طبقه بندها برای بهبود دقت در تشخیص حملات استفاده شده است. نتایج حاصل از اجرای روش درنرمافزار متلب نشان داد که دقت کلی مدل ارایه شده نسبت به دقت هریک از الگوریتم ها به تنهاییبالاتر بوده است. به کارگیری این روش در سیستم های تشخیص نفوذ میتواند عملکرد بالاتری بهمنظور جلوگیری از حملات نسبت به سایر روشهای موجود از خود نشان دهد.

کلمات کلیدی:
سیستم تشخیص نفوذ، کاهش ویژگی، ترکیب طبقه بندها، بهبود دقت

لینک ثابت مقاله در پایگاه سیویلیکا: