عنوان مقاله:
ارایه یک روش جدید تشخیص نفوذ در شبکه های کامپیوتری با استفاده از تکنیک ترکیب درخت تصمیم وشبکه عصبی

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

تعداد صفحات اصل مقاله: 22

نویسندگان:
علی یگانه - *دانشگاه آزاد اسلامی واحد دزفول،گروه کامپیوتر،دزفول،ایران*

مجتبی علیزاده - *رییس مرکز آپا وعضو هیت علمی دانشگاه لرستان*

خلاصه مقاله:
امروزه توسعه روزافزون شبکه های رایانه ای و کاربرد وسیع آن در زندگی بشر، لزوم تامین امنیت این شبکه ها را بیش ازپیش نمایان ساخته است. جهت تامین امنیت از ابزار و تجهیزات مختلفی استفاده می شود که سیستم تشخیص نفوذ از جملهآنها به شمار میرود. مشخص نمودن الگوهای در حجم زیاد داده، کمک بسیار بزرگی به ما می کند. روشهای دادهکاوی با مشخص نمودن یک برچسب دودویی (بسته نرمال، بسته غیرنرمال) و همچنین مشخص نمودن ویژگی ها وخصیصه با الگوریتم های دسته بندی می توانند داده غیرنرمال تشخیص دهند. از همین رو دقت و درستی سیستم هایتشخیص نفوذ افزایش یافته و در نتیجه امنیت شبکه بالا می رود. در این پژوهش، روشی پیشنهادی ارایه می شود که در آنابتدا با استفاده از درخت تصمیم چند برچسبی ویژگی های شاخص و برجسته داده های اولیه مشخص میشوند و سپس بااستفاده از شبکه عصبی پرسپترون چند لایه، داده های کاهش یافته به شبکه آموزش داده میشوند. برای مقایسه نتایجخروجی، بهترین دقت تشخیص حمله DOS با 59 ٪ و کمترین دقت برای حمله PROBE با 78 ٪ بوده است. این نتایجدر مقابل دیگر آثار پیشین در مورد داشتن دقت بالای تخمین در مورد همه ی حملات مختلف بدون آنکه هیچ یک ازآنها در حد پایینی قرار نگرفته اند قابل توجه است. ارزیابی بر اساس مجموعه داده های NSL-KDD انجام گرفته است.

کلمات کلیدی:
تشخیص نفوذ (حمله)، یادگیری باناظر، تخمین چندکلاسه، درخت تصمیم