عنوان مقاله:
ارائه ی یک مدل جهت بهبود تشخیص ناهنجاری در سیستمهای تشخیص نفوذ با مطالعه ی موردی حملات پروب

محل انتشار:
پنجمین همایش بین المللی مهندسی فناوری اطلاعات، کامپیوتر و مخابرات ایران (سال: 1400)

تعداد صفحات اصل مقاله: 17

نویسندگان:
زینب امیری چلمه سرا - *گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد رشت، رشت، ایران*

مرضیه اسداله زاده - *گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد لاهیجان، لاهیجان، ایران*

خلاصه مقاله:
سیستمهای کامپیوتری مبتنی بر شبکه نقش مهمی در جامعه ی امروز ایفا میکنند، از طرفی آنها هدف، خراب کاران و مجرمان قرار گرفته اند . با توسعه ی اینترنت، امنیت شبکه یک فاکتور ضروری در فناوری اطلاعات محسوب میگردد. بنابراین نقش سیستم ها ی تشخیص نفوذ به عنوان ابزارهای ویژه برای شناسایی ناهنجاری و حملات شبکه مشخص است و این شناسایی با جمع آوری اطلاعات از یک یا چند سرور و شبکه و تجزیه و تحلیل داده های جمع آوری شده ممکن می شود. تکنیکها ی یادگیری عمیق برای کشف، تجزیه و تحلیل داده های حجیم و استفاده از الگوهای مفید کاربرد دارند. در این پژوهش یک روش جهت شناسایی حملات بویژه حمله پروب در شبکه پیشنهاد میگردد. طرح پیشنهادی با رویکرد باز آموزش پذیری نمونه های مناسب از ویژگیهای منتخب سعی در انتخاب دقیق تر ویژگیها دارد. فرآیند انتخاب ویژگیها با وزندهی الگوریتم ماشین بردار پشتیبان و جستجوی خطی مقدار آستانه انجام می پذیرد تا یک بردار بهینه جهت آموزش پذیری توسط الگوریتم یادگیری عمیق آماده نماید. نتایج بدست آمده از ارزیابیهای پژوهش دقت ۹۹,۴۹ درصدی روی مجموعه ی بیست درصد آموزش و ۹۸,۷۸ درصدی روی مجموعه ی پیش فرض تست، تشخیص و افتراق صحیح حملات پروب از حملات داس را نشان میدهد.

کلمات کلیدی:
سیستم تشخیص نفوذ، حملات پروب، یادگیری عمیق، وزندهی ماشین بردار پشتیبان