عنوان مقاله:
ارایه یک راهکار دو مرحله ای مبتنی بر یادگیری عمیق به منظور افزایش دقت سیستم های تشخیص نفوذ در شبکه

محل انتشار:
هفتمین همایش مهندسی برق مجلسی (سال: 1397)

تعداد صفحات اصل مقاله: 8

نویسندگان:
علی بهمنی - *دانشجوی کارشناسی ارشد، واحد خوراسگان، دانشگاه آزاد اسلامی، اصفهان، ایران*

سیدامیرحسن منجمی - *دانشیار، دانشگاه اصفهان، اصفهان، ایران*

خلاصه مقاله:
سیستم تشخیص نفوذ یکی از مهمترین المان های امنیتی شبکه های رایانه ای مدرن است که با بررسی سلسله رویدادهای مختلف توانایی شناسایی نفوذ در شبکه را خواهد داشت. این سیستم بطور مستقل(مانند (Snort یا همراه با تجهیزات امنیتی مختلف (مانند Antivirus وUTM و...) در شبکه مورد استفاده قرار می گیرد و بر مبنای دو تکنیک تشخیص رفتار غیر عادی و تشخیص مبتنی بر امضاء می تواند وقوع یک حمله را تشخیص دهد. در حال حاضر بیشترین تحقیقات در خصوص سیستم های تشخیص نفوذ در حوزه تشخیص مبتنی بر رفتار غیرعادی و با استفاده از تکنیک های مختلف (آماری، هوش مصنوعی، داده کاوی، یادگیری ماشین) انجام شده است. در این پژوهش ما با استفاده از انتخاب یک کلاس کاندید از ویژگی های دیتاست KDD و تکنیک یادگیری عمیق توانستیم به یک میزان موثر Accuracy دست پیدا نماییم.

کلمات کلیدی:
سیستم تشخیص نفوذ، امنیت شبکه، یادگیری عمیق