Journal of New Achievements in Electrical, Computer and Technology
Vol. 2, No. 3, Jun-Sep 2022,(49- 64)
WWW.JNAECT.IR

مجله دستاوردهای نوین در برق،کامپیوتر و فناوری
دوره۲، شماره ۳، تابستان ۱۴۰۱ (۶۴-۴۹)

مروری بر الگوریتم های یادگیری عمیق به کار برده شده در سیستم های تشخیص نفوذ

مهشید صالحی[1*]

دپارتمان مهندسی کامپیوتر،واحد مشهد، دانشگاه ازاد اسلامی ، مشهد،ایران salehy.md@gmail.com

چکیده

پیشرفت های سریع در زمینه اینترنت و ارتباطات باعث افزایش زیادی در اندازه شبکه و داده های مربوط به ان شده است. در نتیجه، بسیاری از حملات جدید در حال ایجاد هستند و امنیت شبکه را برای شناسایی دقیق نفوذها با چالش هایی مواجه کرده اند. علاوه بر این، حضور هکر ها با هدف انجام حملات مختلف در داخل شبکه را نمی توان نادیده گرفت. سیستم های تشخیص نفوذ یک ابزار حفاظتی مهم برای تشخیص نفوذ در شبکه است. سیستم های تشخیص نفوذ طبقه بندی کننده ای است که رکورد های ورودی را دریافت و کلاس انواع حملات را پیش بینی می کند. در حملات شبکه الگوریتم‌های مختلف یادگیری عمیق وجود داشته است که برای اجرای سیستم های تشخیص نفوذ پیشنهاد شده است. در دهه‌های گذشته، محققان از یادگیری عمیق مختلفی با رویکردهایی برای طبقه‌بندی و تشخیص ترافیک غیرعادی از ترافیک نرمال در شبکه بدون قبلی دانش قبلی در مورد الگوی حملات استفاده کردند. در این مقاله مروری بر سیستم های تشخیص نفوذ از دیدگاه یادگیری عمیق است. یک بخش جداگانه را به ارائه مجموعه داده های استفاده شده در زمینه سیستم های تشخیص نفوذ به طور خاص، دو مجموعه داده اصلی، KDDCup99 وNSL-KDD اختصاص می دهیم. همچنین معیار های ارزیابی و ابزار های پیاده سازی در سیستم های تشخیص نفوذ مورد بررسی قرار می گیرند.

واژه‌های کلیدی: سیستم های تشخیص نفوذ، یادگیری عمیق ، امنیت شبکه.

.