تشخیص حملات توزیع شده اجتناب از سرویس در شبکه نرم افزاری به کمک یادگیری عمیق

دانشجو: محمد پویا افشاری

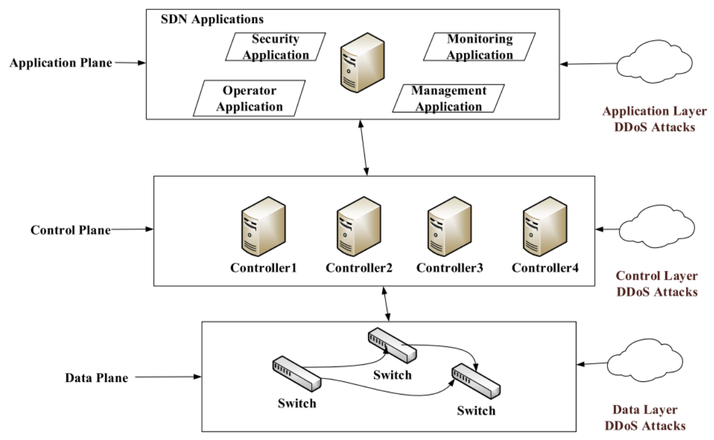
استاد راهنما: دکتر ناصر یزدانی

دانشکده مهندسی برق و کامپیوتر، دانشگاه تهران

مقدمه / خلاصه

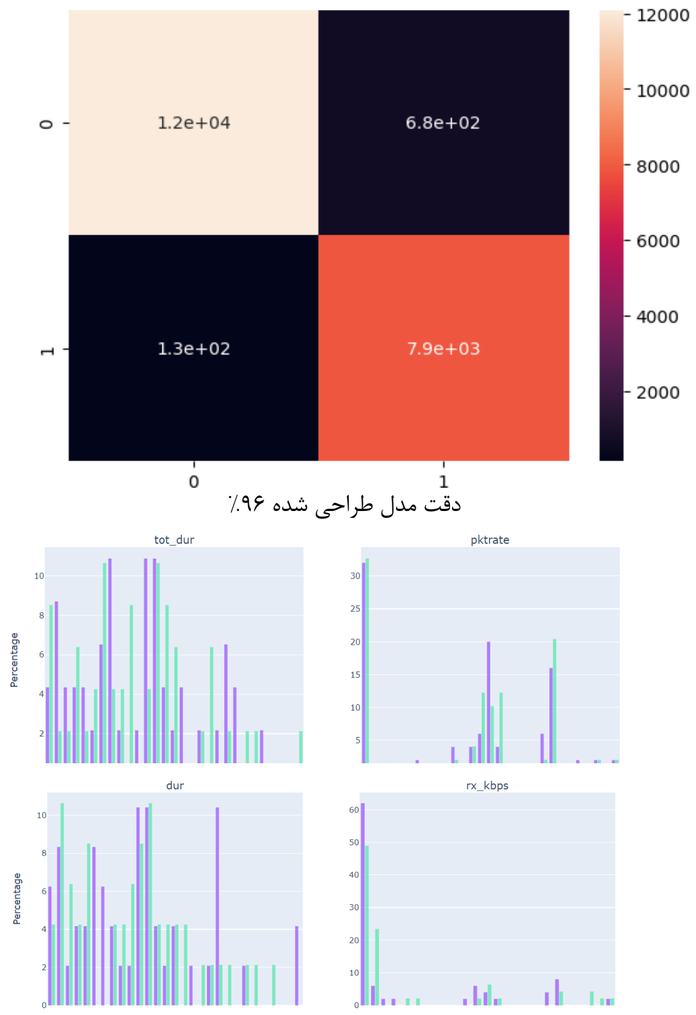
حمله اجتناب سرویس به عنوان تهدید در حوزه امنیت شبکه به خصوص شبکه نرم افزاری برداشت می‌شود که در صورت وقوع منجر به خرابی زیرساخت و سرویس سازمان خواهد شد. هدف از این تحقیق تولید و پیاده سازی مدل خودکار برای تشخیص و تفکیک ویژگی‌های ترافیک عادی و خطرناک در محیط شبکه نرم افزاری و بررسی عملکرد مدل تحت حمله است. همچنین سعی شده به کمک ایجاد داده مصنوعی مدل طراحی شده را برای طیف بزرگ تری از انواع سناریوها آماده کرد.

روش/ساختار/مدل پیشنهادی



مسئله به سه قسمت شکسته می‌شود.

- بخش اول، شامل بدست آوردن مجموعه دادگان برچسب زده شده از ترافیک با ویژگی‌های مختلف و ساخت مدل شبکه کانولوشن می‌شود.
- بخش دوم، بهبود مدل ارائه شده با تغییر پارامترها و ساختار مدل می‌شود. به علاوه به کمک شبکه‌ای که داده‌ی مصنوعی با دقت خوبی از مجموعه دادگان تولید می‌کند می‌توانیم به افزایش کارایی مدل کمک کنیم.



دقت مدل طراحی شده ٪۹۶

ارتباط ستونهای مختلف به ازای داده‌های دیتاست و داده‌های مصنوعی تولید شده

- بخش سوم، نقطه اتصال مدل طراحی شده در سناریو واقعی حاصل می‌شود. در این حالت ما از مدل طراحی شده خروجی می‌گیریم. همچنین محیط شبکه نرم افزاری مرتبط را ایجاد می‌کنیم و از نمونه تشخیص حمله خروجی می‌گیریم.

نتایج

به کمک مدل‌های هوش مصنوعی می‌توان معیارهای متناسب برای کنترل ترافیک شبکه‌های نرم افزاری مختلف ارائه کرد. به این ترتیب نیاز دخالت انسانی در بررسی و کنترل ترافیک شبکه به صورت دستی به حداقل می‌رسد. در این تحقیق به کمک مدل طراحی شده قادر به تشخیص و طبقه بندی ترافیک و انواع مخاطره در شبکه ساخته شده شدیم.

جمع بندی

با توجه به اینکه شبکه نرم افزاری کنترل بهتری روی انواع ترافیک شبکه ایجاد می‌کند اما وجود کنترل کننده مرکزی به مورد خطر قرار گرفتن آن در برابر انواع حملات از جمله حمله اجتناب سرویس اضافه می‌کند. در این تحقیق در گام نخست، مدل شبکه عصبی طراحی شده است که ویژگی‌های مهم ترافیک از هر کلاس ترافیک ورودی را تفکیک می‌کند. در ادامه برای بهبود مدل طراحی شده پارامترهای آن را بهینه کرده و از داده‌های ایجاد شده توسط شبکه مولد متخاصم برای جامع تر کردن خروجی‌ها استفاده کردیم. در نهایت از مدل طراحی شده در سناریو عملی شبکه برای ارزیابی عملکرد استفاده کردیم.

کاربرد های صنعتی:
به کمک مدل تولید شده می‌توان با دقت بالا برای انواع شبکه در صنعت بسته به نیاز و ترافیک ورودی سازمان در تشخیص ترافیک حمله استفاده نمود.

مراجع اصلی

1. D. Kreutz, F. M. V. Ramos, P. Esteves, C. E. Rothenberg, S. Azodolmolky, S. Uhlig, “Software-Defined Networking: A Comprehensive Survey” in proceeding of the IEEE, vol. 103, issue no.1.
2. K. RT, S. T. Selvi, K. Govindarajan, “DDoS detection and analysis in SDN-based environment using support vector machine classifier”, in International Conference on Advance Computing ICAC, 2014, pp. 205-210.
3. S. Dong, K. Abbas, R. Jain, “A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments” in IEEE Access, vol. 7.